TECHNISCHE ARCHITECTUURBLAUWDRUK NETWERK

Datum	12-08-2022
Status	Final
Versie	1.0
Auteur	René Hoogvliet

COLOFON

Titel	Technische architectuurblauwdruk Netwerk
Versie | datum	1.0 | 12 augustus 2022
Samengesteld door	René Hoogvliet Solution Architect Quality BV (namens gemeente Gooise Meren)
Projectcode GM	N.v.t.
Laatste versie bewerkt door	René Hoogvliet

Documentbeheer

Vindbaarheid

De digitale bron van dit document is te vinden op Intranet Gooise Meren ('Implementatie Netwerkvervanging').

Revisie historie

Versie	Datum	Omschrijving	Auteur(s)
0.1	17-06-2022	Eerste opzet en vulling van het document t.b.v. het richting geven aan LCM-acties op de netwerk infrastructuur nodes van de gemeente.	René Hoogvliet
0.9	26-07-2022	Uitwerking van openstaande onderwerpen t.o.v. versie 0.1. Verwerking van reviewcommentaar vanuit de gemeente op versie 0.1. Verwerking van aanvullende opmerkingen uit project overleggen in juni en juli 2022.	René Hoogvliet
1.0	12-08-2022	Verwerking van reviewcommentaar op versie 0.9 van Vincent van Eijden. Dit is de finale versie dat de doelarchitectuur beschrijft binnen de scope van de aanbesteding *Netwerkvervanging Gemeente Gooise Meren*. Deze versie bevat tevens enkele *placeholders* voor onderwerpen die in een latere fase invulling krijgen.	René Hoogvliet

Distributielijst

Naam	Functie	Actie [review | ter info]	Afdeling/organisatie
Carlo van Venrooij	Project Manager	Review	I&A/ Gooise Meren
Vincent van Eijden	Engineer	Review	I&A/ Gooise Meren
Alexander Zagkotsis	CISO	Review	Gooise Meren

Contactlijst

Naam	Functie	Contactgegevens	Afdeling/organisatie
René Hoogvliet	Solution Architect	rene.hoogvliet@quality.nl	Quality BV
Martijn Vuik	Solution Architect	martijn.vuik@quality.nl	Quality BV

Goedkeuring

Dit document is geldig indien goedgekeurd en ondertekend.

Naam	Functie	Datum	Versie	Handtekening
Carlo van Venrooij	Project Manager		1.0	

Inhoudsopgave

1. Introductie en achtergrond

1.1 Werken onder architectuur

Met het 'werken onder architectuur' wordt ervoor gezorgd, dat losse onderdelen in hun samenhang worden ontworpen, zowel op het niveau van de business, de informatievoorziening als de technische middelen.
Een architectuurblauwdruk bevat een samenhangende beschrijving van de door gemeente Gooise Meren gebruikte en geleverde ICT-services, informatie-uitwisseling en infrastructurele onderdelen. Het stelt daarmee de kaders voor ontwerp en beheer. Samenwerking en het bereiken van een gezamenlijk doel op het niveau van de business is de voornaamste reden, waarbij de beginselen, grondslagen en richtlijnen op het gebied van architectuur worden gedragen door het senior management.

1.2 Architectuurblauwdruk

In deze architectuurblauwdruk wordt het domein Netwerk beschreven.

Welke doelstelling heeft een architectuurblauwdruk?
In deze blauwdruk worden de volgende onderwerpen beschreven:

- De vertaling van eisen van de gemeente Gooise Meren op het niveau van de business en informatievoorziening (o.b.v. visie, doelstellingen en strategie) naar een **doelarchitectuur** voor de technische netwerkinfrastructuur.
- De architectuurbouwblokken waaruit het te beschrijven architectuurdomein Netwerk is opgebouwd.
- De standaarden (architectuureisen) die bij het ontwerpen van de netwerkarchitectuur dienen te worden toegepast. De beschreven/geïllustreerde onderdelen worden door architectuureisen gevolgd.
- De architectuureisen die de richtlijnen meegeven bij het opstellen van onderliggende functionele (FO/ HLD) en technische ontwerpen (TO/ LLD).

Wat zijn architectuureisen?
Architectuureisen zijn richtinggevend op het gebied van de (technische) architectuur. Deze zijn gebaseerd op:

- Beleid (en business architectuurprincipes) vanuit de organisatie, aangedragen door belanghebbenden vanuit de business en vertaald naar de technische eigenschap van de infrastructuur,
- Informatie-architectuurprincipes vanuit de organisatie, aangedragen door belanghebbenden vanuit de informatievoorziening, en vertaald naar de technische eigenschap van de infrastructuur,
- Technische architectuurprincipes vanuit de organisatie, aangedragen door belanghebbenden vanuit de techniek, en vertaald naar de technische eigenschap van de infrastructuur.

Vastgestelde architectuureisen in dit document zijn als volgt vormgegeven:

Architectuureis <ID-nr.> - <Onderwerp | Naam>	
[<ID-nr.>.<volgnr.>]	[Beschrijving van de architectuureis | architectuur sub-eis.]

Alle architectuureisen zijn in *Bijlage A: Totaaloverzicht architectuureisen domein Netwerk* gegroepeerd opgenomen.

Wat zijn architectuur bouwblokken[1]?

Architectuur bouwblokken zijn entiteiten binnen een (domein)architectuur die services bieden aan hun omgeving. Een bouwblok kan:

- zelfstandig services leveren aan de omgeving,
- interactie hebben met één of meerdere andere bouwblokken om services te realiseren,
- samengesteld zijn uit meerdere (andere) bouwblokken binnen een architectuurdomein,
- onderdeel uitmaken van een groter samengesteld bouwblok,
- (bij voorkeur) herbruikt worden,
- op diverse manieren samengesteld worden zonder de specifieke kenmerken en interfaces van het bouwblok te veranderen.

Een bouwblok wordt onderkend door domeinexperts als aparte entiteit vanwege:

- de samenhang in, of tussen, de functies die het heeft, en/of
- de set diensten die het levert.

Een bouwblok heeft:

- expliciet en eenduidig te definieren grenzen,
- specifieke funcies, kenmerken en eigenschappen,
- interfaces via welke interactie met aanpalende bouwblokken plaatsvindt.

Een bouwblok is *loosely coupled* met de architectuuromgeving.

De opdeling van een architectuurdomein in bouwblokken is specifiek voor een bepaalde organisatie of bedrijf. Echter, een goede opdeling van een architectuur in bouwblokken levert voordelen op bij integratie van en interoperabiliteit tussen systemen. Tevens vergroot een goede opdeling flexibiliteit bij de realisatie van systemen en applicaties.

De in dit document onderkende bouwblokken worden in de volgende tabelvorm beschreven of samengevat:

Bouwblok - <naam>	
(Beknopte) Conceptuele beschrijving van het bouwblok	*[Beknopte conceptuele beschrijving van het bouwblok. Bv. waaruit bestaat het bouwblok? Welk doel dient het? Welke interfaces heeft het bouwblok? Op welke wijze vindt interactie met de omgeving plaats?]*
Functies van het bouwblok	*[Beschrijving van de functies die het bouwblok heeft en waardoor het services kan realiseren.]*
Services dat het bouwblok biedt (aan de omgeving)	*[Beschrijving van de services die het bouwblok realiseert en die kunnen worden geconsumeerd door andere architectuur componenten (objecten, bouwblokken, etc.).]*
Kwaliteitskenmerken	*[Beschrijving van de (kwaliteits)eisen en beperkingen in termen van security, schaalbaarheid, performance, beschikbaarheid, beheerbaarheid, etc.]*
Relatie met omgeving	*[Beschrijving van de eventuele afhankelijkheid van, of van de relatie met, andere bouwblokken (Bv. af te nemen services van andere bouwblokken binnen de architectuur) en de reden/ oorzaak/ doelstelling ervan.]*

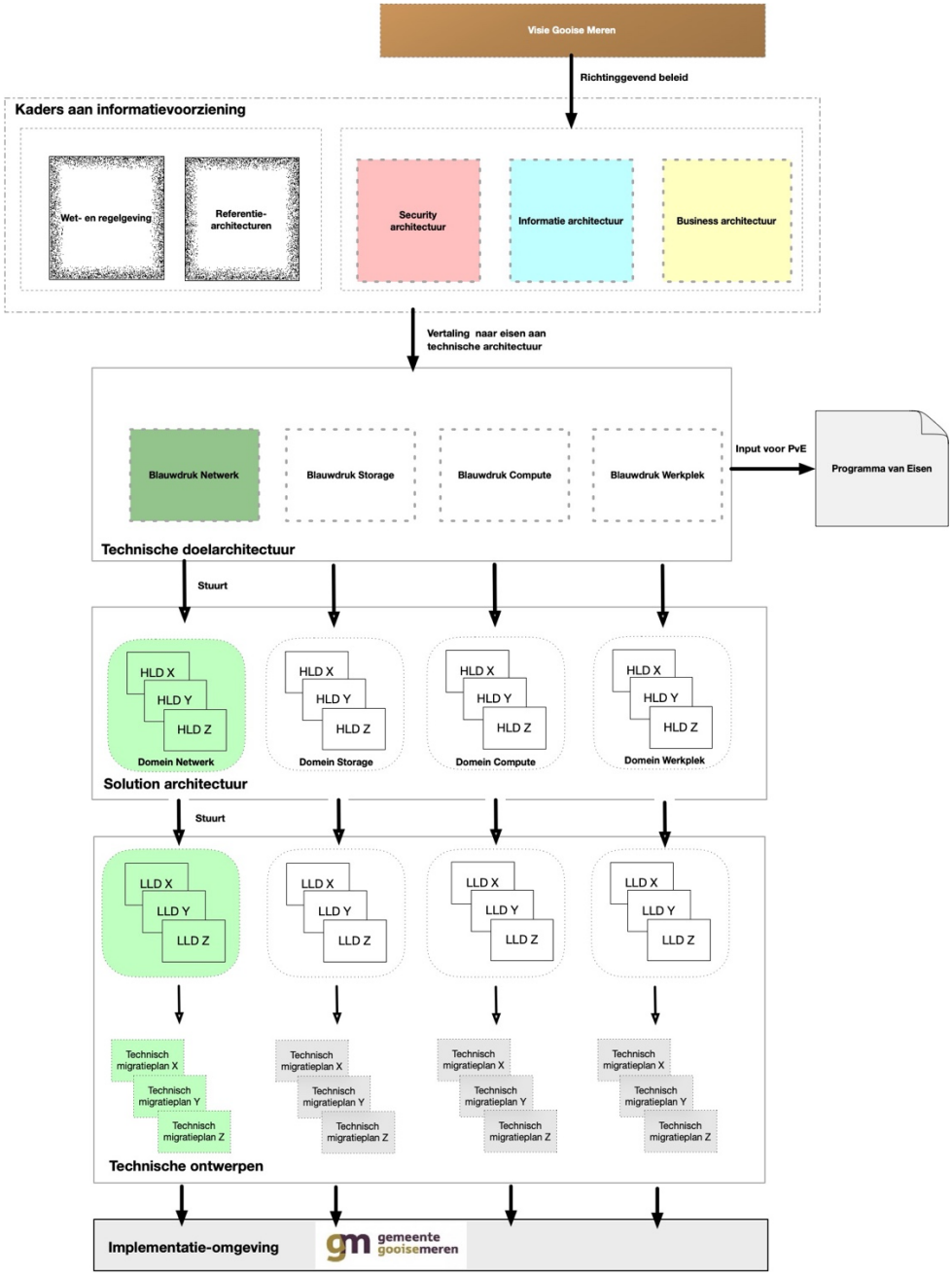
[1] *Met referte aan https://pubs.opengroup.org/architecture/togaf9-doc/arch/ ; Part IV - Architecture Content Framework, 33.Building Blocks*

1.3 Positie van de architectuurblauwdruk Netwerk

In onderstaande Figuur 1-1 is de positie van deze architectuurblauwdruk *Netwerk* (in donkergroen) afgebeeld in relatie tot andere documentatie op het gebied van de Enterprise Architectuur. Een architectuurblauwdruk:

- wordt gebruikt als management- en stuurinstrument (o.b.v. de gedefinieerde architectuureisen die afgeleid zijn uit de visie van de gemeente),
- vormt de basis voor afgeleide ontwerpdocumentatie, en
- levert input in het kader van vervolgtrajecten (e.g. RfP-trajecten).

Door in alle afgeleide documentatie de architectuureisen uit de architectuurblauwdruk als leidraad te nemen, zijn alle functioneel en technisch uitgewerkte onderdelen herleidbaar tot aan de betreffende architectuureisen in deze architectuurblauwdruk. Op deze manier ontstaat een consistent architectuurlandschap, waarbij onderdelen in samenhang worden ontworpen. Dit geldt zowel binnen een architectuurdomein als in relatie tot aanpalende domeinen.
Een visie is niet statisch, zodat ook de architectuurblauwdruk niet als 'statisch' dient te worden beschouwd. Daar waar nodig zal de architectuurblauwdruk, binnen de gestelde kaders, worden aangepast zodra de visie dit afdwingt.



Figuur 1-1 Positie technische architectuurblauwdruk Netwerk.

1.4 Scope architectuurblauwdruk

Deze architectuurblauwdruk beschrijft de diverse services die geleverd worden door de te onderscheiden (architectuur) bouwblokken in het architectuurdomein *Netwerk*. Bij deze beschrijving worden architectuureisen gedefinieerd die van toepassing zijn op de netwerkinfrastructuur van de gemeente.

1.5 Belanghebbenden architectuurblauwdruk

Onderstaande tabel geeft een overzicht van de belanghebbenden (i.e. stakeholders) bij deze blauwdruk.

Tabel 1-1 Overzicht belanghebbenden

Belanghebbenden	Concerns	Invloed (R,A,S,C,I)[2]
Manager FIA (Financien, Informatisering, Automatisering S. Nijs	Kwaliteit digitale dienstverlening.	A (gedelegeerd)
Wethouder Financiën, Jeugd, Onderwijs, Democratische vernieuwing en Dienstverlening G.J. Hendriks	Kwaliteit digitale dienstverlening.	A
Projectleider I & A C. van Venrooij	Tijdige realisatie van kwalitatief juiste deliverables t.b.v. doorontwikkeling van de netwerk architectuur van de gemeente.	R
Netwerk en systeembeheerder V. van Eijden	Conformiteit met de technische doelarchitectuur voor domein Netwerk. Beheerbaarheid van de doelarchitectuur.	C
Senior inkoopadviseur E. Sluis	Conformiteit met wet- en regelgeving rond aanschaf ICT-middelen. Conformiteit lopende contracten.	S, I
Gegevensbeveiliger (CISO) A. Zagkotsis	Conformiteit met de security doelarchitectuur. Conformiteit met wet- en regelgeving rond informatiebeveiliging.	C

1.6 Doelgroep

Doelgroepen van dit document zijn:

- Leden van projectgroepen belast met ontwerp, migratie, transitie en oplevering van de in dit document beschreven architectuur.
- Projectverantwoordelijken voor de acceptatie, uitrol en inrichting.
- Leden van de beheerorganisatie van gemeente Gooise Meren.
- Externe leveranciers verantwoordelijk voor het leveren van diensten aan gemeente Gooise Meren.

1.7 Leeswijzer

De architectuurblauwdruk bestaat uit de volgende onderdelen:

- **Hoofdstuk 1: Introductie en achtergrond**
  Dit hoofdstuk bevat een inleiding bij de architectuurblauwdruk. De onderbouwing van 'het waarom?' van het bestaan van een blauwdruk, de link met het Werken onder Architectuur en de doelgroepen voor wie een dergelijk document geschreven is, worden kort toegelicht. Tevens worden onderdelen als scope van de architectuurblauwdruk en de belanghebbenden behandeld.

[2] *RASCI = Responsible (verantwoordelijk), Accountable (eindverantwoordelijk), Supportive (ondersteunend), Consulted (geraadpleegd), Informed (geïnformeerd).*

- **Hoofdstuk 2: Sites en Services**
  Dit hoofdstuk bevat een beknopt overzicht van de netwerkdiensten en de locaties waar de gemeente deze diensten levert aan haar eindgebruikers/ klanten.

- **Hoofdstuk 3: Technische architectuur - Netwerk**
  In dit hoofdstuk worden de diverse modules binnen de gemeentelijke ICT-infrastructuur beschreven en de bouwblokken, die binnen deze modules onderkend worden en tot het architectuurdomein Netwerk behoren.

- **Hoofdstuk 4: Technische architectuur – Beveiliging**
  In dit hoofdstuk worden de security- alsmede beheer-gerelateerde architectuureisen beschreven die van toepassing zijn op het domein Netwerk.

- **Bijlage A: Totaaloverzicht architectuureisen domein Netwerk**
  Deze bijlage bevat een gegroepeerd overzicht van alle architectuureisen die in dit document zijn beschreven. Dit voor het overzicht, zodat:
  - per topic in één oogopslag de betreffende eisen kunnen worden achterhaald, en
  - de gehele set als input kan dienen voor een Programma van Eisen (PvE) in het kader van een Aanbesteding.

- **Bijlage B: Gebruikte afkortingen**
  Deze bijlage bevat een lijst met afkortingen die gebruikt worden in dit document.

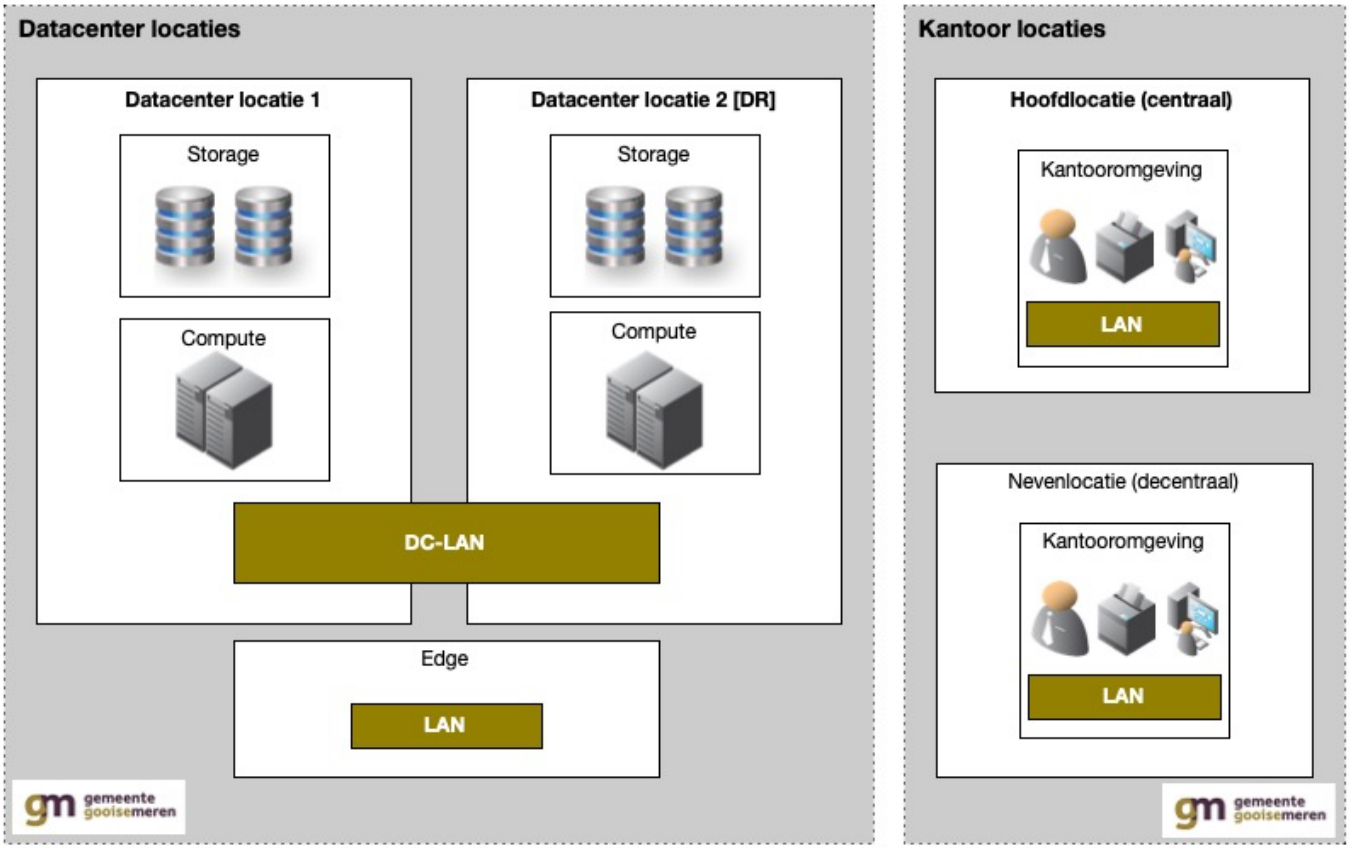
1.8 Relatie met andere documenten/brondocumentatie

Document/bronbestand	Status [concept | definitief]	Auteur
Projectopdracht Vervanging netwerkinfrastructuur	Definitief	Carlo van Venrooij
Functionele eisen netwerkvervanging	N.v.t. (bron: emailbericht dd. 14-02-2022))	Carlo van Venrooij, Vincent van Eijden
PDC-SLA Managed Services (Gooise Meren)	Concept (v0.3)	Nienke Boomkamp (SLTN IT Services BV)
Plan van Aanpak blauwdruk netwerk (Gooise Meren)	Definitief (v0.99)	Martijn Vuik (Quality BV)
Eisenlijst GM – Netwerk infrastructuur	Concept (v0.5)	René Hoogvliet (Quality BV)

2. Sites en services

2.1 Globaal overzicht netwerk infrastructuur

In onderstaande Figuur 2-1 is schematisch weergegeven welke typen locatie er zijn binnen de gemeentelijke ICT-infrastructuur. Tot de scope van deze architectuurblauwdruk behoren de LAN- en DC-LAN-infrastructuren op de locaties van de gemeente Gooise Meren.



Figuur 2-1 Overzicht typen locatie van gemeente Gooise Meren

De volgende typen locatie zijn te onderkennen binnen de ICT-infrastructuur:

- Datacenter locatie.
  Op dit type locatie zijn workloads (i.e. applicaties, informatiesystemen, etc.) ondergebracht op de storage en compute platformen in het on-premises datacenter.
  Er zijn datacenter locaties gerealiseerd in een MER binnen dezelfde fysieke gebouwen die dienst doen als gemeentehuis in Bussum en Hilversum. De locatie in Bussum geldt als de primaire datacenter locatie; de locatie in Hilversum als disaster recovery (DR) faciliteit.
  Een datacenter locatie bevat tevens de LAN-infrastructuur waarmee connectiviteit tussen het on-premises DC-LAN en andere netwerken gerealiseerd is. Deze LAN-infrastructuur vormt hiermee de perimeter (of Edge) van het datacenter netwerk.
- Kantoorlocatie.
  Op dit type locatie zijn kantooromgevingen gerealiseerd waarin eindgebruikers toegang hebben tot ICT-faciliteiten (e.g. werkplek, printer, etc.).

Er bestaan 2 sub-typen Kantoorlocatie: *centraal* en *decentraal*. Het sub-type *centraal* is gerealiseerd in hetzelfde fysieke gebouw als waar de primaire datacenter locatie is ingericht.

2.2 Overzicht netwerkdiensten

In de onderstaande tabellen is een overzicht weergegeven van de diensten die door de netwerk-infrastructuur van de gemeente worden geleverd.

Dienst	**Bedrade netwerktoegang kantoor**
Omschrijving van de service	Deze dienst zorgt ervoor, dat eindgebruikers via hun ICT-devices veilig toegang hebben tot de netwerkinfrastructuur van de gemeente teneinde ICT-diensten te kunnen consumeren. Deze dienst zorgt er tevens voor, dat gebouwgebonden ICT-middelen (e.g. multifunctionele printers of apparatuur voor video conferencing) veilig toegang hebben tot het netwerk.
Verzorgingsgebied	(Netwerk access laag op) Kantoorlocaties
Beschikbaarheid	99,8% (tijdens kantooruren)
Beveiliging van de dienst	Toegang wordt verleend op basis van functionele behoeftes van de afnemers/gebruikers en vigerende security policies van de gemeente. Deze security policies zijn gebaseerd op kenmerken van de eindgebruikers (i.e. digitale identiteit) en/ of het device dat toegang zoekt tot het netwerk.

Dienst	**Draadloze netwerktoegang kantoor**
Omschrijving van de service	Deze dienst zorgt ervoor, dat eindgebruikers via hun ICT-devices veilig en onbedraad toegang hebben tot de netwerkinfrastructuur van de gemeente teneinde ICT-diensten te kunnen consumeren.
Verzorgingsgebied	(Wireless access point gekoppeld aan de netwerk access laag op) Kantoorlocaties
Beschikbaarheid	99,8% (tijdens kantooruren)
Beveiliging van de dienst	Toegang wordt verleend op basis van functionele behoeftes van de afnemers/gebruikers en vigerende security policies van de gemeente. Toegang verloopt op basis van de WPA-2 of -3 standaard in *enterprise* mode. Deze security policies zijn gebaseerd op kenmerken van de eindgebruikers (i.e. digitale identiteit) en/ of het device dat toegang zoekt tot het netwerk.

Dienst	**Netwerktoegang datacenter**
Omschrijving van de service	Deze dienst zorgt ervoor, dat infrastructuurnodes die ondergebracht zijn op één van de (on-premises) datacenterlocaties van de gemeente, veilig toegang hebben tot de gemeentelijke ICT-infrastructuur.
Verzorgingsgebied	(Netwerk access laag op) On-premises datacenter locaties
Beschikbaarheid	99.9%.
Beveiliging van de dienst	Toegang wordt verleend op basis van functionele behoeftes van de te ontsluiten ICT-services/workloads en vigerende security policies van de gemeente. Alleen infrastructuurnodes die door of namens de gemeente worden beheerd en/of anderszins worden vertrouwd, kunnen toegang krijgen tot het datacenternetwerk.

Dienst	**INTRA-Netwerkconnectiviteit**
Omschrijving van de service	Deze dienst zorgt ervoor, dat er communicatiestromen mogelijk zijn (o.b.v. het Ethernet- en/of IP-protocol) tussen: • ICT-devices binnen een door of namens de gemeente beheerde netwerkinfrastructuur op een locatie (e.g. kantoorlocatie of on-premises datacenter), of

Dienst	INTRA-Netwerkconnectiviteit
	• ICT-devices in dergelijke netwerkinfrastructuren die zich op verschillende locaties bevinden.
Verzorgingsgebied	(On-premises) datacenter locaties en kantoorlocaties
Beschikbaarheid	99,9%.
Beveiliging van de dienst	In de door de gemeente beheerde netwerkinfrastructuur zijn securityvoorzieningen aanwezig waarmee beveiligingspolicies worden toegepast op de communicatiestromen, die gefaciliteerd worden door deze service. Deze policies (e.g. encryptie, packet filtering, path isolation, etc.) zijn gebaseerd op de aard van de getransporteerde data (i.e. dataclassificatie) en het vigerend securitybeleid.

Dienst	EXTRA-Netwerkconnectiviteit
Omschrijving van de service	Deze dienst zorgt ervoor, dat er communicatiestromen mogelijk zijn (o.b.v. het IP-protocol) tussen een ICT-device in een door of namens de gemeente beheerde netwerk- infrastructuur op een locatie en een ICT-device in een *niet* door of namens de gemeente beheerde netwerkinfrastructuur (e.g. het netwerk van een externe leverancier). Connectiviteit tussen dergelijke infrastructuurlocaties wordt als een *managed* dienst afgenomen van een service provider. Het koppelvlak met de ICT-infrastructuur van de gemeente voor deze dienst ligt hierbij te allen tijde in een on-premises datacenter locatie.
Verzorgingsgebied	(On-premises) datacenterlocaties
Beschikbaarheid	99,9%
Beveiliging van de dienst	In de door de gemeente beheerde netwerkinfrastructuur zijn securityvoorzieningen aanwezig waarmee beveiligingspolicies worden toegepast op de communicatiestromen, die gefaciliteerd worden door deze service. Deze policies (e.g. encryptie, packet filtering, proxying, etc.) zijn gebaseerd op de aard van de getransporteerde data (i.e. dataclassificatie) en vigerend securitybeleid.

Dienst	INTERNET connectiviteit
Omschrijving van de service	Deze dienst zorgt ervoor, dat er communicatiestromen mogelijk zijn (o.b.v. het IP-protocol) tussen een ICT-device in de door of namens de gemeente beheerde netwerk infrastructuur op een on-premises datacenter locatie en een ICT-voorziening op het Internet. Deze netwerkconnectiviteit met het Internet wordt als een *managed* dienst afgenomen van een Internet Service Provider (ISP). Het koppelvlak met de ICT-infrastructuur van de gemeente voor deze dienst ligt hierbij te allen tijde in een on-premises datacenter locatie.
Verzorgingsgebied	(On-premises) datacenterlocaties
Beschikbaarheid	99,9%
Beveiliging van de dienst	In de door de gemeente beheerde netwerkinfrastructuur zijn securityvoorzieningen aanwezig waarmee beveiligingspolicies worden toegepast op de communicatiestromen, die gefaciliteerd worden door deze service. Deze policies (e.g. encryptie, packet filtering, proxying, etc.) zijn gebaseerd op de aard van de getransporteerde data (i.e. dataclassificatie) en vigerend securitybeleid.

[Onderstaande beschrijving van de 'externe netwerktoegang eindgebruiker' service is een **placeholder** en valt nu buiten scope.]

Dienst	**Externe netwerktoegang eindgebruiker**
Omschrijving van de service	*[Beknopte conceptuele beschrijving van het bouwblok. Bv. waaruit bestaat het bouwblok? Welk doel dient het? Welke interfaces heeft het bouwblok? Op welke wijze vindt interactie met de omgeving plaats?]*
Verzorgingsgebied	*[Beschrijving van de functies die het bouwblok heeft en waardoor het services kan realiseren.]*
Beschikbaarheid	*[Beschrijving van de services die het bouwblok realiseert en die kunnen worden geconsumeerd door andere architectuur componenten (objecten, bouwblokken, etc.).]*
Beveiliging van de dienst	*[Beschrijving van de (kwaliteits)eisen en beperkingen in termen van security, schaalbaarheid, performance, beschikbaarheid, beheerbaarheid, etc.]*

Architectuureis NW-01 - Beschikbaarheid netwerkdiensten	
NW-01.1	Bedrade toegang tot het netwerk in een kantoorlocatie heeft een beschikbaarheidseis van 99,8% (tijdens kantooruren).
NW-01.2	Onbedrade toegang tot het netwerk in een kantoorlocatie heeft een beschikbaarheidseis van 99,8% (tijdens kantooruren).
NW-01.3	Bedrade toegang tot het netwerk in een on-premises datacenter locatie heeft een beschikbaarheidseis van 99,9% (24x7).
NW-01.4	Intra-netwerk connectiviteit (binnen een fysieke locatie of via een WAN-connectie tussen fysieke locaties van de gemeente) heeft een beschikbaarheidseis van 99,9% (24x7).
NW-01.5	Extra-netwerk connectiviteit heeft een beschikbaarheidseis van 99,9% (24x7).
NW-01.6	Internet connectiviteit heeft een beschikbaarheidseis van 99,9% (24x7).

Architectuureis NW-02 – Inzet *managed* diensten	
NW-02.1	Internet connectiviteit wordt als *managed* OSI Laag-3 dienst afgenomen van een externe provider. Het fysieke koppelvlak, dat een dergelijke dienst termineert, bevindt zich op een on-premises datacenter locatie.
NW-02.2	Extranet connectiviteit wordt als *managed* OSI laag-3 dienst afgenomen van een externe provider. Het fysieke koppelvlak, dat een dergelijke dienst termineert, bevindt zich op een on-premises datacenter locatie.
NW-02.3	Intranet connectiviteit (tussen twee fysieke locaties van de gemeente) wordt bij voorkeur als een managed OSI laag-2 afgenomen, tenzij: • dit uit het oogpunt van informatieveiligheid onwenselijk is en tot risico's leidt die niet afdoende gemitigeerd kunnen worden; of • dit economisch gezien ongunstig is; of • dit technisch gezien ongewenst is (e.g. omdat het netwerktopologisch kan leiden tot inefficiënt gebruik van netwerkpaden (lees: STP- blokkades)); of • het connectiviteit betreft tussen datacenter locaties; in dit geval wordt (*private*) connectiviteit o.b.v. *dark fibre* ingezet. Het fysieke koppelvlak dat een dergelijke dienst termineert, bevindt zich (behalve uiteraard een datacenter-interconnect verbinding) op een on-premises datacenter locatie en een decentrale locatie van de gemeente.

3. Technische architectuur - Netwerk

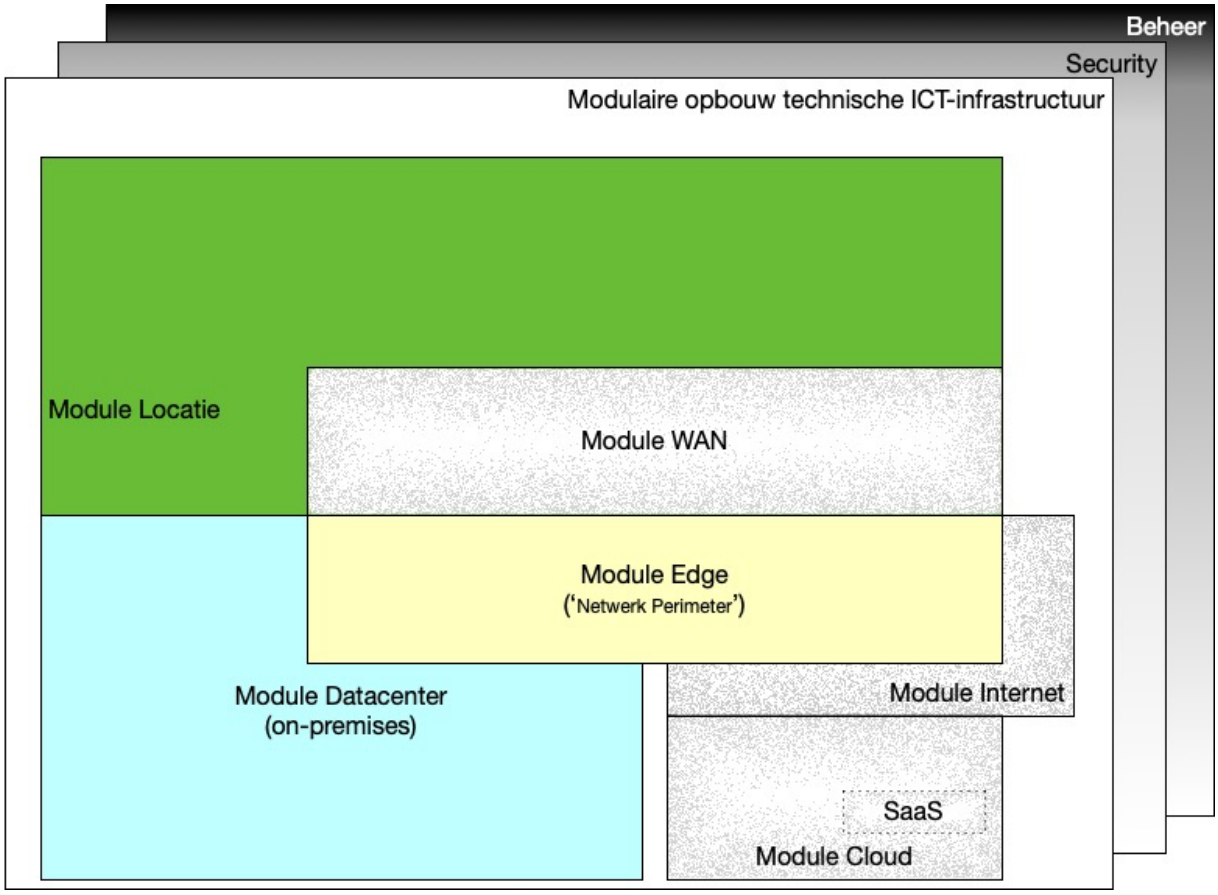
3.1 Modules en bouwblokken

De ICT-infrastructuur van de gemeente Gooise Meren is modulair opgebouwd. Het generieke model van deze modulaire opbouw is afgebeeld in de onderstaande Figuur 3-1.

De modulaire opbouw van de ICT-infrastructuur schept de basis die ervoor zorgt, dat deze infrastructuur:

- Voorspelbaar,
- Gestandaardiseerd,
- Beheerbaar,
- Betrouwbaar, en
- Veilig.

is.



Figuur 3-1 Overzicht modules binnen de ICT-infrastructuur.

In de onderstaande paragrafen van dit hoofdstuk zullen de diverse modules en bouwblokken op het niveau van het architectuurdomein *Netwerk* nader beschreven worden.

3.2 Module Datacenter

De module Datacenter bevat het netwerk-gerelateerde bouwblok Datacenter Netwerk met daarbinnen de sub-bouwblokken:

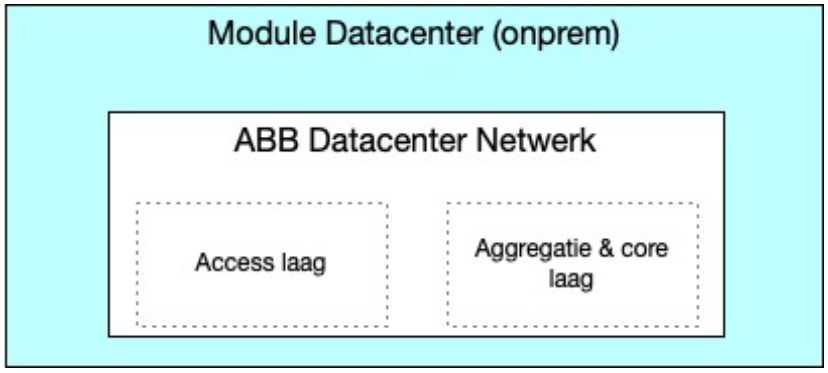
- Access-laag, en
- Aggregatie & core laag.

Gezamenlijk vormt een implementatie van beide sub-bouwblokken het DC-LAN.

Onderstaande Figuur 3-2 bevat een schematische weergave van de module Datacenter (on-premises) en de bouwblokken op het niveau van architectuurdomein Netwerk.

Het Datacenter Netwerk levert:

- via sub-bouwblok 'Access laag' netwerktoegang aan compute en storageplatformen die in het on-premises datacenter zijn ondergebracht,
- via sub-bouwblok 'Aggregatie & core laag' connectiviteitservices naar in- en externe netwerken (via de module Edge (met referte aan paragraaf 3.3)).



Figuur 3-2 Overzicht module Datacenter (on-premises).

Onderstaande tabellen geven een beschrijving van het bouwblok Datacenter Netwerk en de erop van toepassing zijnde architectuureisen.

Bouwblok – Datacenter Netwerk	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het bouwblok Datacenter Netwerk ontsluit platformen in het on-premises datacenter, waarop ICT-workloads (e.g. applicaties en informatiesystemen) zijn ondergebracht, naar de netwerkinfrastructuur. Het datacenter netwerk (ofwel DC-LAN) is daartoe opgebouwd uit de sub-bouwblokken Access laag en Aggregatie & core laag. De DC-LAN-infrastructuren op de twee datacenter locaties van de gemeente zijn verbonden via een datacenter-interconnect verbinding.
Functies van het bouwblok	• Verlenen van fysieke netwerktoegang aan infrastructuurnodes, • Transporteren van verkeersstromen, • Markeren van verkeersstromen, • Prioriteren van verkeersstromen (via classificatie), • Versleutelen van verkeersstromen, • Logisch segmenteren van de fysieke netwerkinfrastructuur, • Isoleren van verkeersstromen.
Services dat het bouwblok biedt (aan de omgeving)	• Datacenter netwerktoegang, • (OSI L2 + L3) Connectiviteitservices.

Bouwblok – Datacenter Netwerk	
Kwaliteitskenmerken	Het bouwblok Datacenter Netwerk biedt garanties voor de beschikbaarheid van de geleverde netwerkdiensten die gebaseerd zijn op prestatiedoelstellingen uit SLAs. Deze garanties zijn het resultaat van redundantie op het niveau van hardwarematige (i.e. middels samenstelling van netwerknodes en fysieke verbindingen tussen nodes) en softwarematige configuraties van componenten binnen het bouwblok. Transport van data is geoptimaliseerd door het aanbrengen van QoS-technieken waarmee markering, classificatie en prioritering van en tussen typen verkeersstromen mogelijk is. Op netwerknodes binnen het bouwblok Datacenter Netwerk zijn protocollen en/of technieken geconfigureerd, waarmee isolatie van endpoints/workloads in het DC-LAN en segmentatie van verkeersstromen over het DC-LAN bewerkstelligd kan worden op basis van het vigerende beleid rond informatiebeveiliging. Verkeersstromen van en naar het datacenter netwerk verlopen via een centrale PEP-functie, die ondergebracht is in het on-premises datacenter, opdat security policies afgedwongen kunnen worden. Het datacenter netwerk biedt connectiviteitsdiensten t.b.v. disaster recovery voorzieningen in de ICT-infrastructuur, doordat: • er een tweede datacenter locatie is ingericht voor specifiek dit doel en • er sprake is van een datacenter-interconnect tussen de primaire en secundaire datacenter locaties. De netwerknodes uit het bouwblok Datacenter Netwerk worden centraal beheerd door services, die geleverd worden vanuit het bouwblok Centrale Netwerk Management Voorziening (met referte aan paragraaf 4.4), teneinde beveiliging en kwaliteit van de vanuit het datacenter netwerk geleverde services te kunnen garanderen.
Relatie met omgeving	Verkeersstromen van en naar: • externe netwerken (i.e. partner netwerken of het Internet) en • interne netwerken, die onder beheerregime vallen van de gemeente, maar geografisch gescheiden zijn van een datacenter locatie, verlopen via de access-nodes in module Edge.

Architectuureis NW-03 - Generieke kenmerken Datacenter Netwerk	
NW-03.1	Nodes in sub-bouwblok Aggregatie & core laag van het bouwblok Datacenter Netwerk ontsluiten: • zowel de access-nodes van het bouwblok Locatie Netwerk (type Centraal), • als access-nodes van het bouwblok Datacenter Netwerk, • als access nodes uit het bouwblok Edge Netwerk.
NW-03.2	Het toe te passen medium tussen netwerknodes in het bouwblok Edge Netwerk en het bouwblok Datacenter Netwerk (i.e. in sub-bouwblok Aggregatie & core laag) is koper.
NW-03.3	Het toe te passen medium tussen netwerknodes in sub-bouwblok Access laag en sub-bouwblok Aggregatie & core laag van het bouwblok Datacenter Netwerk is koper.
NW-03.4	Het toe te passen medium tussen netwerknodes binnen sub-bouwblok Aggregatie & core laag van bouwblok Datacenter Netwerk is koper.

Architectuureis NW-03 - Generieke kenmerken Datacenter Netwerk	
NW-03.5	De ontsluiting van een netwerknode in sub-bouwblok Aggregatie & core laag naar de access-laag (Locatie Netwerk – type Centraal) bestaat uit minimaal 2x fysieke uplinkconnectie (minimaal 10 Gbit/s per connectie).
NW-03.6	Per netwerknode in sub-bouwblok Aggregatie & core laag is sprake van één logische downlink naar de access laag (Locatie Netwerk – type Centraal). Deze logische downlinkconnectie wordt middels linkbundelingstechnologie vormgegeven.
NW-03.7	De ontsluiting van een netwerknode in sub-bouwblok Aggregatie & core laag naar de access-laag binnen het bouwblok Datacenter Netwerk bestaat uit minimaal 2x fysieke uplink connectie (minimaal 10 Gbit/s per connectie).
NW-03.8	Per netwerknode in sub-bouwblok Aggregatie & core laag is sprake van één logische downlink naar de access- laag van het bouwblok Datacenter Netwerk. Deze logische downlink wordt middels linkbundelingstechnologie vormgegeven.
NW-03.9	De ontsluiting van een netwerknode in het bouwblok Edge Netwerk naar sub-bouwblok Aggregatie & core laag van bouwblok Datacenter Netwerk heeft per fysieke uplinkconnectie minimaal een capaciteit van 10 Gbit/s.
NW-03.10	De capaciteit van de fysieke connectiviteit tussen netwerknodes in sub-bouwblok Aggregatie & core laag van het bouwblok Datacenter Netwerk is minimaal 40 Gbit/s.
NW-03.11	De connectiviteit tussen netwerknodes in sub-bouwblok Aggregatie & core laag van het bouwblok Datacenter Netwerk bestaat uit minimaal 2 fysieke verbindingen.
NW-03.12	OSI-laag 2 netwerkconstructs (e.g. VLAN) dienen beschikbaar gemaakt te kunnen worden 'op' meerdere on-premises datacenter locaties (i.e. 'stretched').
NW-03.13	De beschikbaarheid van de vanuit het Datacenter Netwerk geboden netwerkdiensten is minimaal 99,9%.
NW-03.14	Netwerknodes binnen het bouwblok Datacenter Netwerk dienen virtualisatietechnieken te ondersteunen waarmee logische scheiding van de netwerkinfrastructuur op OSI Laag-2 en OSI Laag-3 niveau te bewerkstelligen is, zodat zonering een end-to-end concept is.
NW-03.15	Netwerknodes binnen het bouwblok Datacenter Netwerk leveren services aan en/of nemen services af uit hun omgeving o.b.v. protocollen die gelden als open standaarden.

Architectuureis NW-04 - Kenmerken access-nodes Datacenter Netwerk	
NW-04.1	Een access-node is redundant verbonden met de ontsluitende/bovenliggende netwerknode(s) binnen sub-bouwblok Aggregatie & core laag.
NW-04.2	Redundantie van uplink/downlinkverbindingen dienen middels linkbundelingstechnologie te kunnen worden vormgegeven.
NW-04.3	De access-poorten van een access-node zijn van het type koper met minimaal de ondersteuning van de interfacesnelheden 1 Gbit/s en 10 Gbit/s.
NW-04.4	Access-nodes hebben 48 access-poorten.
NW-04.5	De uplink/downlinkverbindingen van een access-node naar ontsluitende/bovenliggende node(s) in sub-bouwblok Aggregatie & core laag zijn van het type koper met minimaal de ondersteuning van de interfacesnelheden 10 Gbit/s.
NW-04.6	Access-nodes dienen zowel het IPv4- als IPv6-protocol te ondersteunen.
NW-04.7	Access-nodes dienen Quality of Service (QoS) te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
NW-04.8	Access-nodes dienen protocollen te ondersteunen waarmee informatie over aanpalende nodes op het niveau van OSI-laag 1 en 2 kan worden ingewonnen, waarbij het van belang is open standaarden te kunnen gebruiken.
NW-04.9	Access-nodes zijn voorzien van redundante voedingen.
NW-04.10	Access-nodes dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij (conform actuele best practices) echter wel simultaan gebruik- gemaakt kan worden van alle beschikbare netwerkpaden.
NW-04.11	Access-nodes dienen technieken te ondersteunen t.b.v. softwarematige updates waarmee de continuïteit van de door de nodes geboden diensten maximaal wordt gewaarborgd (i.e ISSU, of gelijkwaardige techniek).

Architectuureis NW-04 - Kenmerken access-nodes Datacenter Netwerk	
NW-04.12	OSI Laag 3 terminatiepunten liggen bij voorkeur op het niveau van de centrale PEP-functionaliteiten, maar in ieder geval binnen het bouwblok Datacenter Netwerk.
NW-04.13	Access-nodes worden bij voorkeur afgenomen van één vendor vanwege: - eenvoud van beheer, - gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), - ter voorkoming van compatibiliteitsissues.
NW-04.14	Access-nodes communiceren met hun omgeving op basis van open standaarden.
NW-04.15	Access-nodes dienen informatie betreffende hun (operationele) werking te kunnen loggen op externe hosts/oplossingen o.b.v. in de markt gangbare methoden en standaarden (e.g. syslog, ReST API, CEF).
NW-04.16	Access-nodes dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van ongeoorloofde koppeling van netwerknodes aan het netwerk (e.g. BPDU guard of gelijkwaardige technieken) (e.g. ter preventie van mac flooding).
NW-04.17	Access-nodes dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van misbruik van toegang tot het netwerk (e.g. dynamic arp protection, DHCP snooping of gelijkwaardige technieken).
NW-04.18	Access-nodes dienen managementprotocollen met ingebouwde beveiligingsfuncties te ondersteunen conform actuele standaarden (e.g. SNMPv3, SSHv2, TLSv1.3). Managementprotocollen zonder ingebouwde beveiligingsfuncties zijn niet toegestaan (e.g. Telnet).
NW-04.19	Access-nodes dienen te beschikken over poorten die geschikt zijn voor het koppelen van netwerkbekabeling middels SFP-gebaseerde modules.
NW-04.20	Access-nodes dienen hun lokale clock te kunnen synchroniseren aan externe referenties/bronnen o.b.v. het NTP-protocol.
NW-04.21	Access-nodes dienen 'name resolution' te kunnen verrichten o.b.v. DNS.
NW-04.22	Access-nodes dienen multicastverkeer te ondersteunen o.b.v. in de markt gangbare en gestandaardiseerde protocollen (e.g. IGMP, PIM).
NW-04.23	Access-nodes dienen het transport van 'jumbo' frames te ondersteunen.
NW-04.24	Access-nodes dienen protocollen of technieken (e.g. SGT of functioneel vergelijkbaar) te ondersteunen waarmee op access-poortniveau beperkingen opgelegd/afgedwongen kunnen worden m.b.t. toegangsrechten tot de netwerkinfrastructuur (opdat micro-segmentatie mogelijk is).
NW-04.25	Access-nodes dienen zowel het RADIUS- als TACACS+ protocol te ondersteunen.
NW-04.26	Access-nodes dienen authenticatie methoden o.b.v. PKI-certificaten te ondersteunen, waarbij uitgifte van deze digitale certificaten via auto-enrollment (i.e. het SCEP protocol) verloopt.
NW-04.27	Access-nodes dienen technieken te ondersteunen waarmee stabiliteit/robuustheid van de control-plane geborgd kan worden (e.g. CoPP of gelijkwaardig).
NW-04.28	Access-nodes dienen de mogelijkheid te bieden om te kunnen worden opgenomen in een software-defined netwerk concept (i.e. 'SDN-ready').
NW-04.29	Access-nodes dienen te beschikken over een separaat OOB-interface voor management doeleinden.
NW-04.30	Beheer van access-nodes vindt zoveel mogelijk plaats vanuit/vanaf een centraal management platform. Dit centrale platform levert diensten voor het: • configureren, • monitoren van de operationele status, en • herstellen van functionaliteit (i.e. middels backup en restore), van netwerknodes.
NW-04.31	Het dient mogelijk te zijn om vanaf een centraal management platform technische configuratie op access nodes af te dwingen (via in de markt gangbare open standaard protocollen (e.g. TLSv1.3, SSHv2, NETCONF, RESTCONF of gelijkwaardig)).

Architectuureis NW-05 - Kenmerken netwerknodes Aggregatie & core laag	
NW-05.1	De ontsluiting tussen netwerknodes in sub-bouwblok Aggregatie & core laag onderling moet een capaciteit hebben van 40 Gbit/s.
NW-05.2	Een netwerk node in sub-bouwblok Aggregatie & core laag dient minimaal te voorzien in een combinatie van 1 Gbit/s en 10 Gbit/s poorten.
NW-05.3	Een netwerk node in sub-bouwblok Aggregatie & core laag voorziet in non-oversubscribed poorten (op elke poort).
NW-05.4	Redundantie van uplink/downlinkverbindingen dient middels linkbundelingstechnologie te kunnen worden vormgegeven
NW-05.5	De poorten van een netwerknode in sub-bouwblok Aggregatie & core laag zijn van het type koper met minimaal de ondersteuning van de interfacesnelheden 1 Gbit/s en 10 Gbit/s.
NW-05.6	Een netwerk node in sub-bouwblok Aggregatie & core laag heeft 48 access-poorten en is bij voorkeur modulair uitbreidbaar.
NW-05.7	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen zowel data-transport o.b.v. het IPv4- als IPv6-protocol te ondersteunen.
NW-05.8	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen Quality of Service (QoS) te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
NW-05.9	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen protocollen te ondersteunen waarmee informatie over aanpalende nodes op het niveau van OSI-laag 1 en 2 kan worden ingewonnen, waarbij het van belang is open standaarden te kunnen gebruiken.
NW-05.10	Netwerknodes in sub-bouwblok Aggregatie & core laag zijn voorzien van redundante voedingen.
NW-05.11	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij (conform actuele best practices) echter wel simultaan gebruikgemaakt kan worden van alle beschikbare netwerkpaden.
NW-05.12	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen technieken te ondersteunen t.b.v. softwarematige updates waarmee continuïteit van de door de nodes geboden diensten maximaal wordt gewaarborgd (i.e ISSU, of gelijkwaardige techniek).
NW-05.13	OSI Laag 3 terminatiepunten liggen bij voorkeur op het niveau van de centrale PEP-functionaliteiten, maar in ieder geval binnen bouwblok Datacenter Netwerk.
NW-05.14	Netwerknodes in sub-bouwblok Aggregatie & core laag worden bij voorkeur afgenomen van één vendor vanwege: - eenvoud van beheer, - gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), ter voorkoming van compatibiliteitsissues.
NW-05.15	Netwerknodes in sub-bouwblok Aggregatie & core laag communiceren met hun omgeving op basis van open standaarden.
NW-05.16	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen informatie betreffende hun (operationele) werking te kunnen loggen op externe hosts/oplossingen o.b.v. in de markt gangbare methoden en standaarden (e.g. syslog, ReST API, CEF).
NW-05.17	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen protocollen te ondersteunen waarmee analyse van het netwerkverkeer mogelijk is (e.g. SPAN of gelijkwaardig).
NW-05.18	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen protocollen te ondersteunen waarmee statistische analyse van het netwerkverkeer mogelijk is (e.g. sFlow, NetFlow, IPFIX of gelijkwaardig).
NW-05.19	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van ongeoorloofde koppeling van nodes aan het netwerk (e.g. BPDU guard of gelijkwaardige technieken).
NW-05.20	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van misbruik van toegang tot het netwerk (e.g. dynamic arp protection, DHCP snooping of gelijkwaardige technieken).
NW-05.21	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen managementprotocollen met ingebouwde beveiligingsfuncties te ondersteunen conform actuele standaarden (e.g. SNMPv3,

Architectuureis NW-05 - Kenmerken netwerknodes Aggregatie & core laag	
	SSHv2, TLSv1.3). Managementprotocollen zonder ingebouwde beveiligingsfuncties zijn niet toegestaan (e.g. Telnet).
NW-05.22	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen te beschikken over poorten die geschikt zijn voor het koppelen van netwerkbekabeling middels SFP-gebaseerde modules.
NW-05.23	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen hun lokale clock te kunnen synchroniseren aan externe referenties/ bronnen o.b.v. het NTP-protocol.
NW-05.24	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen 'name resolution' te kunnen verrichten o.b.v. DNS.
NW-05.25	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen multicast verkeer te ondersteunen o.b.v. in de markt gangbare protocollen (e.g. IGMP, PIM).
NW-05.26	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen in de markt gangbare protocollen te ondersteunen waarmee een netwerknode de 'next hop' bepaalt voor een netwerkpakket, indien een virtuele node (e.g. virtuele router) de next hop is voor het netwerkverkeer (e.g. VRRP).
NW-05.27	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen transport van 'jumbo' frames te ondersteunen.
NW-05.28	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen protocollen of technieken (e.g. SGT, SXP of functioneel vergelijkbaar) te ondersteunen waarmee op access-poort niveau beperkingen opgelegd/ afgedwongen kunnen worden m.b.t. toegangsrechten tot de netwerkinfrastructuur (opdat micro-segmentatie/host-isolation mogelijk is).
NW-05.29	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen zowel het RADIUS- als TACACS+ protocol te ondersteunen.
NW-05.30	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen authenticatie methoden o.b.v. PKI-certificaten te ondersteunen, waarbij uitgifte van deze digitale certificaten via auto-enrollment (i.e. het SCEP protocol) verloopt.
NW-05.31	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen technieken te ondersteunen waarmee stabiliteit/robuustheid van de control-plane geborgd kan worden (e.g. CoPP of gelijkwaardig).
NW-05.32	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen de mogelijkheid te bieden om te kunnen worden opgenomen in een software-defined netwerk concept (i.e. 'SDN-ready').
NW-05.33	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen te beschikken over een separaat OOB-interface voor management doeleinden.
NW-05.34	Beheer van netwerknodes in sub-bouwblok Aggregatie & core laag vindt zoveel mogelijk plaats vanuit vanaf een centraal management platform. Dit centrale platform levert diensten voor het: • configureren, • monitoren van de operationele status, en • herstellen van functionaliteit (i.e. middels backup en restore), van netwerknodes.
NW-05.35	Het dient mogelijk te zijn om vanaf een centraal management platform technische configuratie op netwerknodes in sub-bouwblok Aggregatie & core laag af te dwingen (via in de markt gangbare open standaard protocollen (e.g. TLSv1.3, SSHv2, NETCONF, RESTCONF of gelijkwaardig)).

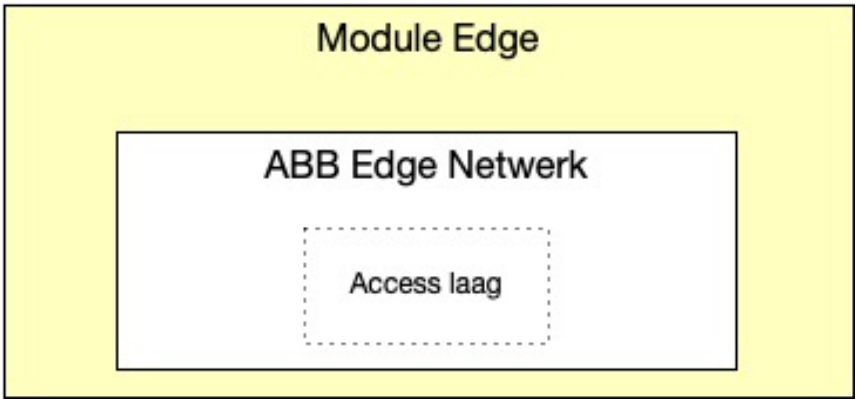
3.3 Module Edge

De module Edge bevat het netwerk-gerelateerde bouwblok Edge Netwerk met daarbinnen het sub-bouwblok Access-laag.

De onderstaande Figuur 3-3 bevat een schematische weergave van de module Edge op het niveau van architectuurdomein *Netwerk*.

Het Edge Netwerk levert:

- diensten t.b.v. INTRA-netwerk/WAN-connectiviteit (i.e. connectiviteit tussen (delen van) netwerkinfrastructuren die onder het technisch beheerregime van de gemeente vallen),
- diensten t.b.v. EXTRA-netwerkconnectiviteit (i.e. connectiviteit van en naar externe partner netwerken), en
- diensten t.b.v. connectiviteit naar het Internet.



Figuur 3-3 Overzicht module Edge.

De onderstaande tabellen geven een beschrijving van bouwblok Edge Netwerk en de erop van toepassing zijnde architectuureisen.

Bouwblok – Edge Netwerk	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het bouwblok Edge Netwerk vormt het koppelvlak voor connectiviteit tussen het on-premises datacenter en: • interne netwerken, die onder het technisch beheerregime van de gemeente vallen, maar geografisch gescheiden zijn van een datacenter locatie (i.e. een instantie van sub-bouwblok Locatie Netwerk – Decentraal (met referte aan paragraaf 3.5.2)), en • externe netwerken, die niet onder het beheerregime van de gemeente vallen.
Functies van het bouwblok	• Verlenen van fysieke netwerktoegang aan netwerknodes die op een on-premises datacenter locatie het fysieke koppelvlak vormen voor ofwel INTRA-netwerk (i.e. WAN) ofwel EXTRA-netwerk ofwel INTERNET connectiviteitsdiensten, • Transporteren van verkeersstromen, • Markeren van verkeersstromen, • Prioriteren van verkeersstromen (via classificatie), • Versleutelen van verkeersstromen, • Logisch segmenteren van de fysieke netwerkinfrastructuur, • Isoleren van verkeersstromen.
Services dat het bouwblok biedt (aan de omgeving)	• INTRA-netwerkconnectiviteit met interne netwerken, die onder het technisch beheerregime van de gemeente vallen, maar geografisch gescheiden zijn van een datacenter locatie, • EXTRA-netwerkconnectiviteit met externe netwerken, die niet onder het beheerregime van de gemeente vallen, • Internet connectiviteit.

Bouwblok – Edge Netwerk	
Kwaliteitskenmerken	Het bouwblok Edge Netwerk biedt garanties voor de beschikbaarheid van de geleverde netwerkdiensten, die gebaseerd zijn op prestatiedoelstellingen uit SLAs. Deze garanties zijn het resultaat van redundantie op het niveau van hardwarematige (i.e. middels samenstelling van netwerknodes en fysieke verbindingen tussen nodes) en softwarematige configuraties van componenten binnen het bouwblok. Transport van data is geoptimaliseerd door het aanbrengen van QoS-technieken waarmee markering, classificatie en prioritering van en tussen typen verkeersstromen mogelijk is. Op netwerknodes binnen bouwblok Edge Netwerk zijn protocollen en/of technieken geconfigureerd, waarmee segmentatie van verkeersstromen over het (DC-)LAN bewerkstelligd kan worden op basis van het vigerende beleid rond informatiebeveiliging. Inkomende verkeersstromen naar het datacenter netwerk verlopen via een centrale PEP-functie, die ondergebracht is in het on-premises datacenter, opdat security policies afgedwongen kunnen worden. Het edge netwerk biedt connectiviteitsdiensten t.b.v. disaster recovery voorzieningen in de ICT-infrastructuur, doordat deze diensten op beide datacenter locaties aanwezig zijn. De netwerknodes uit het bouwblok Edge Netwerk worden centraal beheerd door services die geleverd worden vanuit het bouwblok Centrale Netwerk Management Voorziening (met referte aan paragraaf 4.4), teneinde beveiliging en kwaliteit van de vanuit het edge netwerk geleverde services te kunnen garanderen.

Relatie met omgeving	De access-nodes, waaruit de module Edge is opgebouwd, ontsluiten:
	• netwerknodes (e.g. routers), die op een on-premises datacenter locatie het fysieke koppelvlak vormen voor:
	  ○ ofwel INTRA-netwerk connectiviteitsdiensten (module WAN),
	  ○ ofwel EXTRA-netwerk connectiviteitsdiensten
	  ○ ofwel INTERNET connectiviteitsdiensten (module Internet);
	en deze access-nodes van bouwblok Edge Netwerk worden zelf ontsloten naar:
	• netwerknodes in sub-bouwblok Aggregatie & core laag van bouwblok Datacenter Netwerk.

Architectuureis NW-06 - Generieke kenmerken Edge Netwerk	
NW-06.1	Het bouwblok Edge Netwerk bestaat louter uit access-nodes. Deze nodes zijn fysiek ondergebracht in de on-premises datacenter locaties van de gemeente.
NW-06.2	Nodes in de access-laag van het bouwblok Edge Netwerk ontsluiten: • netwerknodes (e.g. routers) die op een on-premises datacenter locatie het fysieke koppelvlak vormen voor ofwel INTRA-netwerk (i.e. WAN) ofwel EXTRA-netwerk ofwel INTERNET connectiviteitsdiensten; en deze access-nodes van bouwblok Edge Netwerk worden zelf ontsloten naar: • netwerknodes in sub-bouwblok Aggregatie & core laag van bouwblok Datacenter Netwerk.
NW-06.3	Ontsluiting van een netwerknode in de access-laag van het bouwblok Edge Netwerk naar de netwerknodes in sub-bouwblok Aggregatie & core laag (van bouwblok Datacenter Netwerk)

Architectuureis NW-06 - Generieke kenmerken Edge Netwerk	
	bestaat uit minimaal 2x fysieke uplink- connecties o.b.v. koper (minimaal 10 Gbit/s per connectie).
NW-06.4	Per netwerknode in de accesslaag van bouwblok Edge Netwerk is sprake van één logische uplink naar een netwerknodes in sub-bouwblok Aggregatie & core laag (Datacenter Netwerk). Deze logische uplink wordt middels linkbundelingstechnologie vormgegeven.
NW-06.5	De beschikbaarheid van de vanuit het Edge Netwerk geboden netwerkdiensten is minimaal 99,9%.
NW-06.6	Netwerknodes binnen het bouwblok Edge Netwerk dienen virtualisatietechnieken te ondersteunen waarmee logische scheiding van de netwerkinfrastructuur op OSI Laag-2 en OSI Laag-3 niveau te bewerkstelligen is, zodat zonering een end-to-end concept is.
NW-06.7	Netwerknodes binnen het bouwblok Edge Netwerk leveren services aan en/ of nemen services af uit hun omgeving o.b.v. protocollen die gelden als open standaarden.

Architectuureis NW-07 - Kenmerken access-nodes Edge Netwerk	
NW-07.1	Een access-node is redundant verbonden met de ontsluitende/bovenliggende node(s) binnen sub-bouwblok Aggregatie & core laag van het bouwblok Datacenter Netwerk.
NW-07.2	Redundantie van uplink/downlinkverbindingen dient middels linkbundelingstechnologie te kunnen worden vormgegeven
NW-07.3	De access-poorten van een access-node zijn van het type koper of glas met minimaal de ondersteuning van de interfacesnelheden 1 Gbit/s en 10 Gbit/s.
NW-07.4	Access-nodes hebben 48 access-poorten.
NW-07.5	De uplink/downlinkverbindingen van een access-node naar ontsluitende/bovenliggende node(s) in sub-bouwblok Aggregatie & core laag van het bouwblok Datacenter Netwerk zijn van het type koper met minimaal de ondersteuning van de interfacesnelheden 10 Gbit/s.
NW-07.6	Access-nodes dienen zowel datatransport o.b.v. het IPv4- als IPv6-protocol te ondersteunen.
NW-07.7	Access-nodes dienen Quality of Service (QoS) te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
NW-07.8	Access-nodes dienen protocollen te ondersteunen waarmee informatie over aanpalende nodes op het niveau van OSI-laag 1 en 2 kan worden ingewonnen, waarbij het van belang is open standaarden te kunnen gebruiken.
NW-07.9	Access-nodes zijn voorzien van redundante voedingen.
NW-07.10	Access-nodes dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij (conform actuele best practices) echter wel simultaan gebruik- gemaakt kan worden van alle beschikbare netwerkpaden.
NW-07.11	Access-nodes dienen technieken te ondersteunen t.b.v. softwarematige updates waarmee continuïteit van de door de nodes geboden diensten maximaal wordt gewaarborgd (i.e ISSU, of gelijkwaardige techniek).
NW-07.12	OSI Laag 3 terminatiepunten liggen bij voorkeur op het niveau van de centrale PEP-functionaliteiten, maar in ieder geval binnen bouwblok Datacenter Netwerk.
NW-07.13	Access-nodes worden bij voorkeur afgenomen van één vendor vanwege: - eenvoud van beheer, - gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), ter voorkoming van compatibiliteitsissues.
NW-07.14	Access-nodes communiceren met hun omgeving op basis van open standaarden.
NW-07.15	Access-nodes dienen informatie betreffende hun (operationele) werking te kunnen loggen op externe hosts/oplossingen o.b.v. in de markt gangbare methoden en standaarden (e.g. syslog, ReST API, CEF).
NW-07.16	Access-nodes dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van ongeoorloofde koppeling van netwerknodes aan het netwerk (e.g. BPDU guard of gelijkwaardige technieken) (e.g. ter preventie van MAC flooding).

Architectuureis NW-07 - Kenmerken access-nodes Edge Netwerk	
NW-07.17	Access-nodes dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van misbruik van toegang tot het netwerk (e.g. dynamic arp protection, DHCP snooping of gelijkwaardige technieken).
NW-07.18	Access-nodes dienen managementprotocollen met ingebouwde beveiligingsfuncties te ondersteunen conform actuele standaarden (e.g. SNMPv3, SSHv2, TLS)v1.3. Managementprotocollen zonder ingebouwde beveiligingsfuncties zijn niet toegestaan (e.g. Telnet).
NW-07.19	Access-nodes dienen te beschikken over poorten die geschikt zijn voor het koppelen van netwerkbekabeling middels SFP-gebaseerde modules.
NW-07.20	Access-nodes dienen hun lokale clock te kunnen synchroniseren aan externe referenties/bronnen o.b.v. het NTP-protocol.
NW-07.21	Access-nodes dienen 'name resolution' te kunnen verrichten o.b.v. DNS.
NW-07.22	Access-nodes dienen multicastverkeer te ondersteunen o.b.v. in de markt gangbare en gestandaardiseerde protocollen (e.g. IGMP, PIM).
NW-07.23	Access-nodes dienen het transport van 'jumbo' frames te ondersteunen.
NW-07.24	Access-nodes dienen protocollen of technieken (e.g. SGT of functioneel vergelijkbaar) te ondersteunen waarmee op access-poort niveau beperkingen opgelegd/afgedwongen kunnen worden m.b.t. toegangsrechten tot de netwerkinfrastructuur (opdat micro-segmentatie mogelijk is).
NW-07.25	Access-nodes dienen zowel het RADIUS- als TACACS+ protocol te ondersteunen.
NW-07.26	Access-nodes dienen authenticatie methoden o.b.v. PKI-certificaten te ondersteunen, waarbij uitgifte van deze digitale certificaten via auto-enrollment (i.e. het SCEP protocol) verloopt.
NW-07.27	Access-nodes dienen technieken te ondersteunen waarmee stabiliteit of robuustheid van de control-plane geborgd kan worden (e.g. CoPP of gelijkwaardig).
NW-07.28	Access-nodes dienen de mogelijkheid te bieden om te kunnen worden opgenomen in een software-defined netwerk concept (i.e. 'SDN-ready').
NW-07.29	Access-nodes dienen te beschikken over een separate OOB-interface voor managementdoeleinden.
NW-07.30	Het beheer van access-nodes vindt zoveel mogelijk plaats vanuit/vanaf een centraal management platform. Dit centrale platform levert diensten voor het: • configureren, • monitoren van de operationele status, en • herstellen van functionaliteit (i.e. middels backup en restore), van netwerknodes.
NW-07.31	Het dient mogelijk te zijn om vanaf een centraal management platform technische configuratie op access nodes af te dwingen (via in de markt gangbare open standaard protocollen (e.g. TLSv1.3, SSHv2, NETCONF, RESTCONF of gelijkwaardig)).

3.4 Module WAN

De module WAN levert (met referte aan paragraaf 2.2 (NW-01.4 en NW-02.3)) de INTRA-Netwerk connectiviteitservices, waarmee connectiviteit tussen twee fysieke locaties (i.e. gebouwen) wordt gerealiseerd, waarin zich een (deel van de) netwerkinfrastructuur bevindt, dat onder het beheerregime van de gemeente staat.

De netwerknodes, die fysiek het koppelvlak (of demarcatie) van de module WAN vormen, zijn:

- ofwel op een datacenter locatie,
- ofwel op een (decentrale (kantoor))locatie,

van de gemeente ondergebracht.

Deze netwerknodes worden:

- op een datacenter locatie fysiek ontsloten naar een access-node van de module Edge (met referte aan paragraaf 3.3),
- op een (decentrale (kantoor))locatie ontsloten naar een access-node van het bouwblok Locatie Netwerk – type Decentraal (met referte aan paragraaf 3.5.2).

3.5 Module Locatie

De module Locatie bevat het netwerk-gerelateerde bouwblok Locatie Netwerk met daarbinnen de twee sub-bouwblokken:

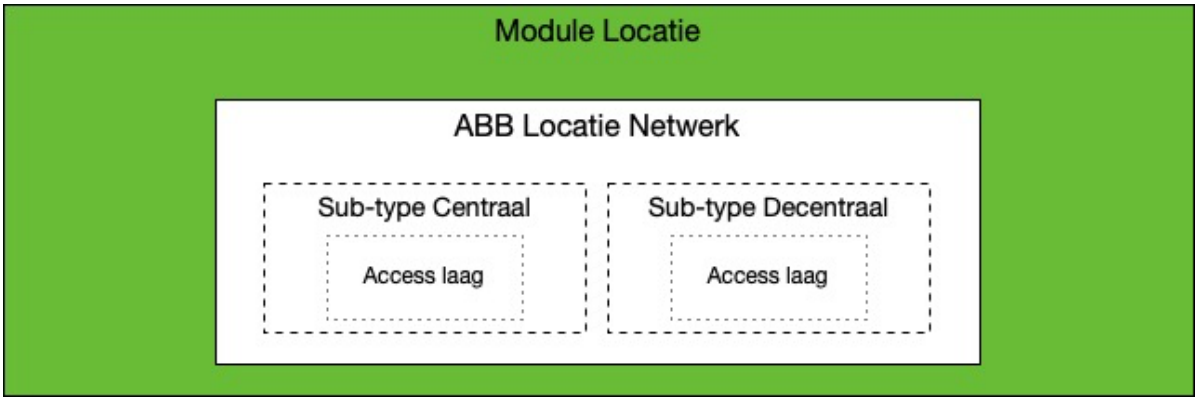
- Centraal, en
- Decentraal.

Beide sub-bouwblokken bestaan louter uit een Access-laag.

De onderstaande Figuur 3-4 bevat een schematische weergave van de module Locatie en de bouwblokken op het niveau van architectuurdomein *Netwerk*.

Het Locatie Netwerk levert:

- netwerktoegang aan eindgebruikerdevices en ICT-systemen, die diensten leveren in de categorie kantoorautomatisering (e.g. multifunctionele printers) op een kantoorlocatie,
- connectiviteit naar het Datacenter Netwerk.

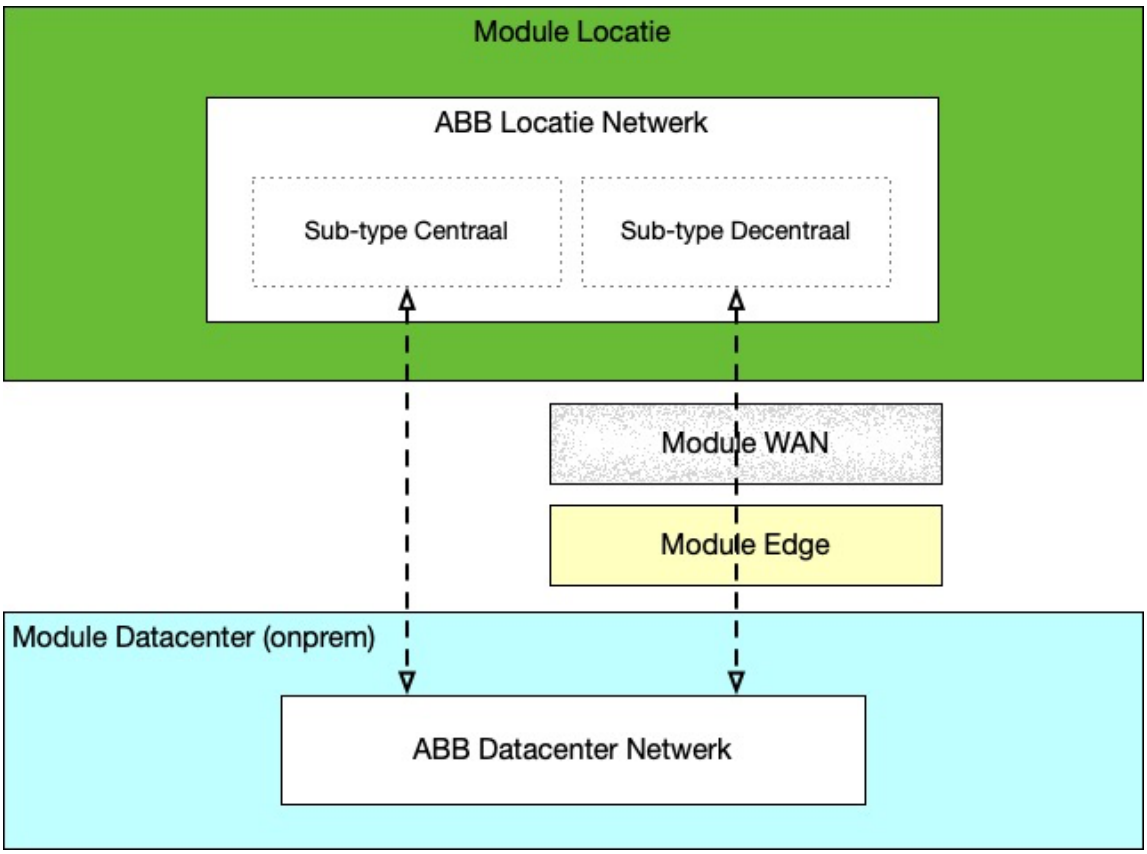


Figuur 3-4 Overzicht module Locatie.

Het onderscheid tussen beide sub-typen van het bouwblok Locatie Netwerk is gebaseerd op de wijze van ontsluiting naar het on-premises datacenter:

- Centraal: het kantoor-LAN van dit sub-type bevindt zich in hetzelfde gebouw als een on-premises datacenter locatie van de gemeente.
- Decentraal: het kantoor-LAN van dit sub-type bevindt zich niet in hetzelfde gebouw als een on-premises datacenter locatie van de gemeente. Connectiviteit vanuit dit type locatie naar het on-premises datacenter verloopt via de modules Edge en WAN (met referte aan paragrafen 3.3 en 3.4).

De onderstaande Figuur 3-5 bevat schematisch het verschil in connectiviteit naar het on-premises datacenter voor de sub-types Decentraal en Centraal van bouwblok Locatie Netwerk.



Figuur 3-5 Verschil in connectiviteit tussen Locatie sub-types Centraal en Decentraal.

De onderstaande tabellen geven een beschrijving van het bouwblok Locatie Netwerk en de erop van toepassing zijnde architectuureisen.

Bouwblok – Locatie Netwerk	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het bouwblok Locatie Netwerk ontsluit op veilige wijze eindgebruikers, hun devices en ICT-systemen, die diensten leveren in de categorie kantoor automatisering (e.g. multifunctionele printers) naar de LAN-infrastructuur op een kantoorlocatie. Beveiliging vindt plaats doordat access-nodes in het LAN pas toegang verlenen, nadat de digitale identiteit van een eindgebruiker, het eindgebruikerdevice of ICT-systeem is gecontroleerd tegen een centrale IAM-service. Eindgebruikers kunnen via hun devices bedraad en onbedraad toegang krijgen tot het netwerk op een locatie. Er wordt onderscheid gemaakt tussen de volgende sub-bouwblokken: • Centraal, waarvan het LAN fysiek in hetzelfde gebouw gevestigd is als het DC-LAN van een on-premises datacenter locatie, en • Decentraal, waarvan het LAN via de modules WAN en Edge ontsloten is naar het DC-LAN van een on-premises datacenter locatie.
Functies van het bouwblok	• Verlenen van netwerktoegang aan eindgebruikers, hun devices en ICT-systemen, die diensten leveren in de categorie kantoorautomatisering, • (sub-type Decentraal:) Verlenen van netwerktoegang aan netwerknodes die behoren tot module WAN, • Transporteren van verkeersstromen, • Markeren van verkeersstromen, • Prioriteren van verkeersstromen (via classificatie),

Bouwblok – Locatie Netwerk	
	• Versleutelen verkeersstromen, • Logisch segmenteren van de fysieke netwerkinfrastructuur, • Isoleren van verkeersstromen.
Services dat het bouwblok biedt (aan de omgeving)	(Bedrade en draadloze) Netwerktoegang voor eindgebruiker devices en ICT-systemen, die diensten leveren in de categorie kantoorautomatisering.(e.g. multifunctionele printers) op een kantoorlocatie; (OSI L2 + L3) Connectiviteitsservices naar het Datacenter Netwerk. Voor een LAN-infrastructuur op een locatie van het sub-type Decentraal geldt dat deze connectiviteit tevens via de module WAN verloopt (met referte aan paragraaf 3.4).
Kwaliteitskenmerken	Het bouwblok Locatie Netwerk biedt garanties voor de beschikbaarheid van de geleverde netwerkdiensten, die gebaseerd zijn op prestatiedoelstellingen uit SLAs. Deze garanties zijn het resultaat van redundantie op het niveau van hardwarematige (i.e. middels samenstelling van netwerknodes en fysieke verbindingen tussen nodes) en softwarematige configuraties van componenten binnen het bouwblok en naar aanpalende modules (i.e. Datacenter (on-prem) in geval van locatie sub-type Centraal en WAN in geval van locatie sub-type Decentraal) . Toegang tot het LAN op een locatie wordt beveiligd middels authenticatie en autorisatie van eindgebruikers en systemen. Hiertoe communiceren access-nodes in het LAN met het bouwblok Centrale Netwerktoegang Verlening (met referte aan paragraaf 4.2.3). Na vaststelling van de digitale identiteit van een eindgebruiker en/ of systeem worden beveiligingspolicies toegepast op de access-node in het LAN. Op netwerknodes binnen het bouwblok Locatie Netwerk zijn verder protocollen en/of technieken geconfigureerd, waarmee segmentatie van verkeersstromen over het LAN bewerkstelligd kan worden op basis van het vigerende beleid rond informatiebeveiliging. Transport van data is geoptimaliseerd door het aanbrengen van QoS-technieken waarmee markering, classificatie en prioritering van en tussen typen verkeersstromen mogelijk is. De netwerknodes uit het bouwblok Locatie Netwerk worden centraal beheerd door services geleved vanuit het bouwblok Centrale Netwerk Management Voorziening (met referte aan paragraaf 4.4), teneinde beveiliging en kwaliteit van de vanuit het LAN op een locatie geleverde services te kunnen garanderen.
Relatie met omgeving	Sub-type Locatie Netwerk - Centraal: access-nodes van het LAN van dit sub-type zijn fysiek direct gekoppeld aan de netwerknodes in sub-bouwblok Aggregatie & core laag van het DC-LAN (Datacenter Netwerk). Sub-type Locatie Netwerk - Decentraal: access-nodes van het LAN van dit sub-type zijn op basis van een INTRA-Netwerkconnectiviteitsservice in de module WAN en via de module Edge ontsloten naar de netwerknodes in sub-bouwblok Aggregatie & core laag van het DC-LAN. De beveiliging van toegang tot de LAN-infrastructuur wordt op basis van het RADIUS-protocol gerealiseerd via afname van de IAM-service die geboden wordt vanuit het bouwblok Centrale Netwerktoegang Verlening.

3.5.1 Locatie Netwerk – type Centraal

Architectuureis NW-08 - Generieke kenmerken Locatie Netwerk [type Centraal]

NW-08.1	Het toe te passen medium tussen netwerknodes in de bouwblokken Locatie Netwerk (i.e. accesslaag van type Centraal) en Datacenter Netwerk (i.e. sub-bouwblok Aggregatie & core laag van het DC-LAN) is koper.
NW-08.2	Ontsluiting van een netwerknode in de access laag (Locatie Netwerk – type Centraal) naar sub-bouwblok Aggregatie & core laag van bouwblok Datacenter Netwerk bestaat uit minimaal 2x fysieke uplink.
NW-08.3	Per netwerk node in de access laag (Locatie Netwerk – type Centraal) is sprake van één logische uplink naar sub-bouwblok Aggregatie & core laag van bouwblok Datacenter Netwerk. Deze logische uplink wordt middels linkbundelingstechnologie vormgegeven.
NW-08.4	Netwerknodes binnen het bouwblok Locatie Netwerk [type Centraal] dienen virtualisatie-technieken te ondersteunen waarmee logische scheiding van de netwerkinfrastructuur op OSI Laag-2 en OSI Laag-3 niveau te bewerkstelligen is, zodat zonering een end-to-end concept is.
NW-08.5	Access nodes leveren services aan en/ of nemen services af uit hun omgeving o.b.v. protocollen die gelden als open standaarden.

Architectuureis NW-09 - Kenmerken access-nodes Locatie Netwerk [type Centraal]	
NW-09.1	Een access-node is redundant verbonden met de ontsluitende/bovenliggende node(s) binnen sub-bouwblok Aggregatie & core laag van bouwblok Datacenter Netwerk.
NW-09.2	Redundantie van uplink/downlinkverbindingen dient middels linkbundelingstechnologie te kunnen worden vormgegeven.
NW-09.3	Uplink/downlinkverbindingen hebben minimaal een capaciteit van 2x 10 Gbit/s.
NW-09.4	De access-poorten van access-nodes zijn van het type koper 10/100/1000 Mbit/s.
NW-09.5	Access-nodes hebben 48 access-poorten.
NW-09.6	Access-nodes dienen te voorzien in Power-over-Ethernet mogelijkheden (o.b.v. de IEEE 802.3at-2009 (PoE+) of een recentere IEEE standaard) om gekoppelde devices (e.g. wireless access points of IP-telefoons) van stroom te kunnen voorzien.
NW-09.7	Access-nodes dienen zowel het IPv4- als IPv6-protocol te ondersteunen.
NW-09.8	Access-nodes dienen Quality of Service (QoS) te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
NW-09.9	Access-nodes dienen protocollen te ondersteunen waarmee informatie over aanpalende nodes op het niveau van OSI-laag 1 en 2 kan worden ingewonnen, waarbij het van belang is open standaarden te kunnen gebruiken.
NW-09.10	Access-nodes zijn voorzien van redundante voedingen.
NW-09.11	Access-nodes dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij (conform actuele best practices) echter wel simultaan gebruik- gemaakt kan worden van alle beschikbare netwerkpaden.
NW-09.12	OSI Laag 3 terminatiepunten liggen bij voorkeur op het niveau van sub-bouwblok Aggregatie & core laag van bouwblok Datacenter Netwerk.
NW-09.13	Access-nodes worden bij voorkeur afgenomen van één vendor vanwege: - eenvoud van beheer, - gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), - ter voorkoming van compatibiliteitsissues.
NW-09.14	Access-nodes communiceren met hun omgeving op basis van open standaarden.
NW-09.15	Access-nodes dienen informatie betreffende hun (operationele) werking te kunnen loggen op externe hosts/ oplossingen o.b.v. in de markt gangbare methoden en standaarden (e.g. syslog, ReST API, CEF).
NW-09.16	Access-nodes dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van ongeoorloofde koppeling van netwerknodes aan het netwerk (e.g. BPDU guard of gelijkwaardige technieken) (e.g. ter preventie van mac flooding).
NW-09.17	Access-nodes dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van misbruik van toegang tot het netwerk (e.g. dynamic arp protection, DHCP snooping of gelijkwaardige technieken).

Architectuureis NW-09 - Kenmerken access-nodes Locatie Netwerk [type Centraal]	
NW-09.18	Access-nodes dienen managementprotocollen met ingebouwde beveiligingsfuncties te ondersteunen conform actuele standaarden (e.g. SNMPv3, SSHv2, TLSv1.3). Managementprotocollen zonder ingebouwde beveiligingsfuncties zijn niet toegestaan (e.g. Telnet).
NW-09.19	Access-nodes dienen technieken te ondersteunen t.b.v. softwarematige updates waarmee continuïteit van de door de nodes geboden diensten maximaal wordt gewaarborgd (i.e ISSU, of gelijkwaardige techniek).
NW-09.20	Access-nodes dienen te beschikken over poorten die geschikt zijn voor het koppelen van netwerkbekabeling middels SFP-gebaseerde modules
NW-09.21	Access-nodes dienen hun lokale clock te kunnen synchroniseren aan externe referenties/bronnen o.b.v. het NTP-protocol.
NW-09.22	Access-nodes dienen 'name resolution' te kunnen verrichten o.b.v. DNS.
NW-09.23	Access-nodes dienen multicastverkeer te ondersteunen o.b.v. in de markt gangbare protocollen (e.g. IGMP, PIM).
NW-09.24	Access-nodes dienen het transport van 'jumbo' frames te ondersteunen.
NW-09.25	Access-nodes dienen (op basis van de IEEE 802.1X standaard) te voorzien in functionaliteit om op access poortniveau dynamisch authenticatie en autorisatie van eindgebruikers en ICT-devices te faciliteren.
NW-09.26	Access-nodes dienen zowel het RADIUS- als TACACS+ protocol te ondersteunen.
NW-09.27	Access-nodes dienen authenticatie methoden o.b.v. PKI-certificaten te ondersteunen, waarbij uitgifte van deze digitale certificaten via auto-enrollment (i.e. het SCEP protocol) verloopt.
NW-09.28	Access-nodes dienen technieken te ondersteunen waarmee stabiliteit of robuustheid van de control-plane geborgd kan worden (e.g. CoPP of gelijkwaardig).
NW-09.29	Access-nodes dienen de mogelijkheid te bieden om te kunnen worden opgenomen in een software-defined netwerk concept (i.e. 'SDN-ready').
NW-09.30	Access-nodes dienen te beschikken over een separate OOB-interface voor management-doeleinden.
NW-09.31	Het beheer van access-nodes vindt zoveel mogelijk plaats vanuit/vanaf een centraal management platform. Dit centrale platform levert diensten voor het • configureren, • monitoren van de operationele status, en • herstellen van functionaliteit (i.e. middels backup en restore), van netwerknodes.
NW-09.32	Het dient mogelijk te zijn om vanaf een centraal management platform technische configuratie op access nodes af te dwingen (via in de markt gangbare open standaard protocollen (e.g. TLSv1.3, SSHv2, NETCONF, RESTCONF of gelijkwaardig)).

3.5.2 Locatie Netwerk – type Decentraal

Architectuureis NW-10 - Generieke kenmerken Locatie Netwerk [type Decentraal]	
NW-10.1	Het toe te passen medium tussen een access-node in het bouwblok Locatie Netwerk (type Decentraal) en een netwerknode, die het fysieke koppelvlak met de INTRA-netwerk (i.e WAN) connectiviteitsdienst vormt, is koper.
NW-10.2	De ontsluiting van een netwerknode in de access laag (Locatie Netwerk – type Decentraal) naar een netwerknode, die het fysieke koppelvlak met de INTRA-netwerk (i.e WAN) connectiviteitsdienst vormt, bestaat (indien mogelijk) uit minimaal 2x fysieke uplink. Alleen de eigenschappen (e.g. geen ondersteuning van linkbundeling of gebrek aan fysieke uplinkpoorten) van de aan een access-node te koppelen netwerknode mogen hierin beperkend zijn.

NW-10.3	Per access node is (indien mogelijk) sprake van één logische uplink naar een netwerknode, die het fysieke koppelvlak met de INTRA-netwerk (i.e WAN) connectiviteitsdienst vormt. Deze logische uplink wordt middels linkbundelingstechnologie vormgegeven.
NW-10.4	Access-nodes binnen het bouwblok Locatie Netwerk [type Decentraal] dienen virtualisatie-technieken te ondersteunen waarmee logische scheiding van de netwerkinfrastructuur op OSI Laag-2 en OSI Laag-3 niveau te bewerkstelligen is, zodat zonering een end-to-end concept is.
NW-10.5	Access-nodes leveren services aan en/ of nemen services af uit hun omgeving o.b.v. protocollen die gelden als open standaarden.

Architectuureis NW-11 - Kenmerken access-nodes Locatie Netwerk [type Decentraal]	
NW-11.1	Een access-node is redundant verbonden met de ontsluitende/bovenliggende node(s).
NW-11.2	Redundantie van uplink/downlinkverbindingen dient middels linkbundelingstechnologie te kunnen worden vormgegeven.
NW-11.3	Uplink/downlinkverbindingen hebben minimaal een capaciteit van 1 Gbit/s.
NW-11.4	De access-poorten van access-nodes zijn van het type koper 10/100/1000 Mbit/s.
NW-11.5	Access-nodes hebben 48 access-poorten.
NW-11.6	Access-nodes dienen te voorzien in Power-over-Ethernet mogelijkheden (o.b.v. de IEEE 802.3at-2009 (PoE+) of een recentere IEEE standaard) om gekoppelde devices (e.g. wireless access points of IP-telefoons) van stroom te kunnen voorzien.
NW-11.7	Access-nodes dienen zowel data-transport o.b.v. het IPv4- als IPv6-protocol te ondersteunen.
NW-11.8	Access-nodes dienen Quality of Service (QoS) te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
NW-11.9	Access-nodes dienen protocollen te ondersteunen waarmee informatie over aanpalende nodes op het niveau van OSI-laag 1 en 2 kan worden ingewonnen, waarbij het van belang is open standaarden te kunnen gebruiken.
NW-11.10	Access-nodes zijn voorzien van redundante voedingen.
NW-11.11	Access-nodes dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij (conform actuele best practices) echter wel simultaan gebruik- gemaakt kan worden van alle beschikbare netwerkpaden.
NW-11.12	Access-nodes worden bij voorkeur afgenomen van één vendor vanwege: - eenvoud van beheer, - gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), - ter voorkoming van compatibiliteitsissues.
NW-11.13	Access-nodes communiceren met hun omgeving op basis van open standaarden.
NW-11.14	Access-nodes dienen informatie betreffende hun (operationele) werking te kunnen loggen op externe hosts/oplossingen o.b.v. in de markt gangbare methoden en standaarden (e.g. syslog, ReST API, CEF).
NW-11.15	Access-nodes dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van ongeoorloofde koppeling van netwerknodes aan het netwerk (e.g. BPDU guard of gelijkwaardige technieken) (e.g. ter preventie van MAC flooding).
NW-11.16	Access-nodes dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van misbruik van toegang tot het netwerk (e.g. dynamic arp protection, DHCP snooping of gelijkwaardige technieken).
NW-11.17	Access-nodes dienen managementprotocollen met ingebouwde beveiligingsfuncties te ondersteunen conform actuele standaarden (e.g. SNMPv3, SSHv2, TLSv1.3). Managementprotocollen zonder ingebouwde beveiligingsfuncties zijn niet toegestaan (e.g. Telnet).
NW-11.18	Access-nodes dienen technieken te ondersteunen t.b.v. softwarematige updates waarmee continuïteit van de door de nodes geboden diensten maximaal wordt gewaarborgd (i.e ISSU, of gelijkwaardige techniek).
NW-11.19	Access-nodes dienen te beschikken over poorten die geschikt zijn voor het koppelen van netwerkbekabeling middels SFP-gebaseerde modules

Architectuureis NW-11 - Kenmerken access-nodes Locatie Netwerk [type Decentraal]	
NW-11.20	Access-nodes dienen hun lokale clock te kunnen synchroniseren aan externe referenties/bronnen o.b.v. het NTP-protocol.
NW-11.21	Access-nodes dienen 'name resolution' te kunnen verrichten o.b.v. DNS.
NW-11.22	Access-nodes dienen multicastverkeer te ondersteunen o.b.v. in de markt gangbare protocollen (e.g. IGMP, PIM).
NW-11.23	Access-nodes dienen het transport van 'jumbo' frames te ondersteunen.
NW-11.24	Access-nodes dienen (op basis van de IEEE 802.1X standaard) te voorzien in functionaliteit om op access poortniveau dynamisch authenticatie en autorisatie van eindgebruikers en ICT-devices te faciliteren.
NW-11.25	Access-nodes dienen zowel het RADIUS- als TACACS+ protocol te ondersteunen.
NW-11.26	Access-nodes dienen authenticatie methoden o.b.v. PKI-certificaten te ondersteunen, waarbij uitgifte van deze digitale certificaten via auto-enrollment (i.e. het SCEP protocol) verloopt.
NW-11.27	Access-nodes dienen technieken te ondersteunen waarmee stabiliteit/ robuustheid van de control-plane geborgd kan worden (e.g. CoPP of gelijkwaardig).
NW-11.28	Access-nodes dienen de mogelijkheid te bieden om te kunnen worden opgenomen in een software-defined netwerk concept (i.e. 'sdn-ready').
NW-11.29	Access-nodes dienen te beschikken over een separate OOB-interface voor management doeleinden.
NW-11.30	Beheer van access-nodes vindt zoveel mogelijk plaats vanuit/ vanaf een centraal management platform. Dit centrale platform levert diensten voor het: • configureren, • monitoren van de operationele status, en • herstellen van functionaliteit (i.e. middels backup en restore), van netwerknodes.
NW-11.31	Het dient mogelijk te zijn om vanaf een centraal management platform technische configuratie op access nodes af te dwingen (via in de markt gangbare open standaard protocollen (e.g. TLSv1.3, SSHv2, NETCONF, RESTCONF of gelijkwaardig)).

3.5.3 Draadloos Locatie Netwerk

[Onderstaande beschrijving is een **placeholder** en valt buiten de scope.]

Bouwblok – Draadloos Locatie Netwerk	
(Beknopte) Conceptuele beschrijving van het bouwblok	*[Beknopte conceptuele beschrijving van het bouwblok. Bv. waaruit bestaat het bouwblok? Welk doel dient het? Welke interfaces heeft het bouwblok? Op welke wijze vindt interactie met de omgeving plaats?]*
Functies van het bouwblok	*[Beschrijving van de functies die het bouwblok heeft en waardoor het services kan realiseren.]*
Services dat het bouwblok biedt (aan de omgeving)	*[Beschrijving van de services die het bouwblok realiseert en die kunnen worden geconsumeerd door andere architectuurcomponenten (objecten, bouwblokken, etc.).]*
Kwaliteitskenmerken	*[Beschrijving van de (kwaliteits)eisen en beperkingen in termen van security, schaalbaarheid, performance, beschikbaarheid, beheerbaarheid, etc.]*
Relatie met omgeving	*[Beschrijving van de eventuele afhankelijkheid van of van de relatie met andere bouwblokken (Bv. af te nemen services van andere bouwblokken binnen de architectuur) en de reden/ oorzaak/ doelstelling ervan.]*

Architectuureis NW-12 – Kenmerken Draadloos Locatie Netwerk	
NW-12.1	[Placeholder.]

4. Technische architectuur - Beveiliging Netwerk

4.1 Beveiliging van netwerkconnectiviteit

[*Beschrijving/ opsomming van de geldende architectuureisen in het kader van security zonering en segmentatie van de netwerkinfrastructuur.*]

[Verdere uitwerking van deze paragraaf is nu buiten scope van de blauwdruk.]

Architectuureis NW-13 - Gebruik van veilige bekabeling voor data-communicatie	
NW-13.1	Netwerkbekabeling dient te voldoen aan actuele ANSI/TIA en/ of ISO/IEC standaarden (e.g. TIA 568, ISO 11801).

Architectuureis NW-14 - Inzet van betrouwbare middelen	
NW-14.1	Netwerknodes in de ICT-infrastructuur dienen actieve ondersteuning te hebben van de leverancier (i.e. OEM) op de hard- en software, waaruit deze nodes zijn opgebouwd. Technische kwetsbaarheden, die de veilige werking van netwerknodes bedreigen, kunnen zo tijdig gemitigeerd worden. Netwerknodes worden vervangen voordat de actieve ondersteuning vervalt.

Architectuureis NW-15 - Versleuteling van datastromen over externe netwerken	
NW-15.1	Datacommunicatie tussen: • een ICT-device binnen een ICT-infrastructuur (die onder het beheerregime valt) van de gemeente en een ICT-device buiten deze infrastructuur, of • twee ICT-devices binnen delen van ICT-infrastructuren (die onder het beheerregime vallen) van de gemeente en dat deels over een extern (i.e. buiten dit beheerregime vallend) netwerk verloopt, wordt te allen tijde versleuteld o.b.v. in de markt veilig geachte open protocollen (e.g. MACsec of IPSEC).

Architectuureis NW-16 - Afdwingen beveiligingspolicies op data-stromen	
NW-16.1	[Placeholder.]

4.1.1 Normenkader voor de netwerkinfrastructuur

[Verdere uitwerking van dit onderwerp is buiten scope : placeholder.]

4.1.2 Security zonering en (micro-)segmentatie

[Verdere uitwerking van dit onderwerp is buiten scope : placeholder.]

4.2 Beveiliging van netwerktoegang

[*Beschrijving/ opsomming van de geldende architectuureisen in het kader van security t.b.v. toegang door eindgebruikers of digitale middelen tot de netwerk infrastructuur.*
Het betreft hier overigens de beveiliging van toegang tot het verlenen van netwerk connectiviteit an sich, en ***niet*** *de beveiliging van toegang tot de diverse digitale (applicatieve) diensten die door de gemeente aan afnemers worden geleverd* ***over*** *deze netwerk infrastructuur.*]
[Placeholder.]

4.2.1 Module Datacenter

[Placeholder.]

4.2.2 Module Edge

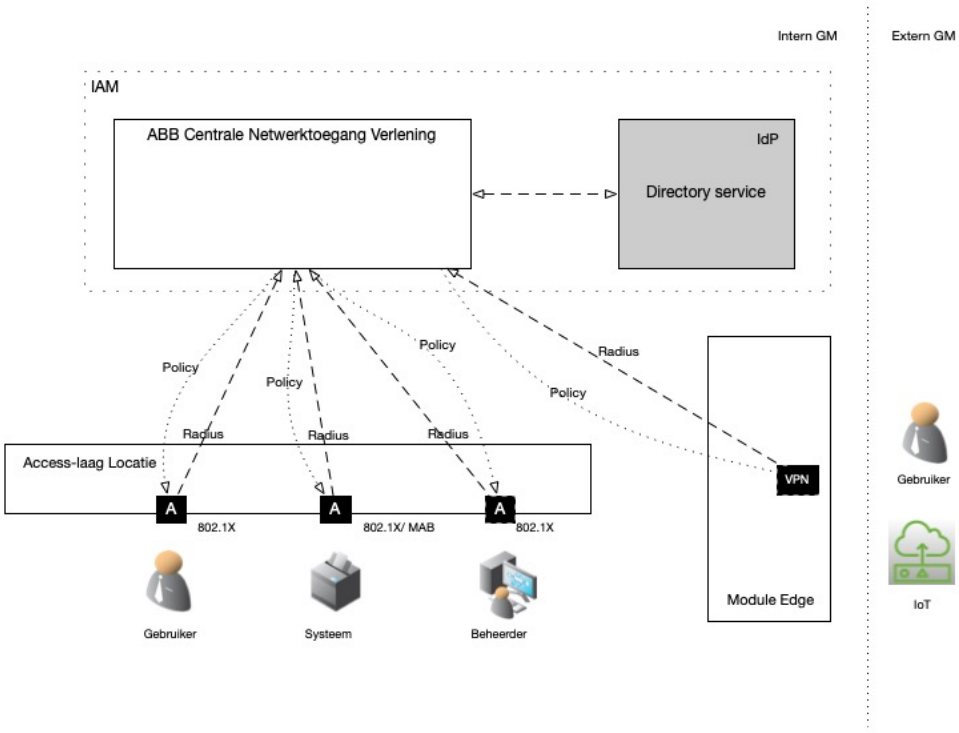
[Placeholder.]

4.2.3 Module Locatie

Binnen de module Locatie levert het bouwblok Centrale Netwerktoegang Verlening (CNV) services voor:

- de identiteitscontrole van, en
- het verlenen van gecontroleerde toegang tot de netwerkinfrastructuur aan,

eindgebruikers en door hen gebruikte ICT-apparatuur.



Figuur 4-1 Conceptuele weergave netwerktoegang (NAC).

Bouwblok – Centrale Netwerktoegang Verlening	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het bouwblok Centrale Netwerktoegang Verlening (CNV) levert services waarmee interne en externe toegang tot de netwerk infrastructuur door eindgebruikers, hun devices en ICT-systemen beveiligd kan worden.

Bouwblok – Centrale Netwerktoegang Verlening	
	Interne netwerktoegang. Bouwblok CNV legt, op basis van de vastgestelde digitale identiteit (i.e. na *authenticatie*) van een eindgebruiker en/ of systeem, dynamisch beveiligingspolicies op aan de access-node in een LAN (i.e. *autorisatie* op netwerk poort niveau van een access-node). Externe netwerktoegang. Bouwblok CNV legt op een VPN head-end device, op basis van de vastgestelde digitale identiteit (i.e. na *authenticatie*) van een eindgebruiker en/ of systeem, dynamisch beveiligingspolicies op aan de VPN tunnelsessie tussen een (eindgebruiker) device/ systeem en het VPN head end device (i.e. *autorisatie* op sessie niveau). Het VPN head-end device bevindt zich hierbij in het on-premises datacenter. Bouwblok CNV biedt functionaliteit voor het samenstellen en dynamisch kunnen toepassen van (complexe) beveiligings-/ toegangspolicies op basis van kenmerken van de digitale identiteit van de toegang verzoekende eindgebruiker en/ of het toegang verzoekende device/ ICT-systeem. Deze kenmerken liggen op het niveau van hardware, software en/ of IAM-accounts. Voor de verificatie van kenmerken van IAM-accounts maakt bouwblok CNV op basis van het RADIUS protocol gebruik van de centrale directory service (IdP) (van de IAM-omgeving) van de gemeente.
Functies van het bouwblok	• Vaststellen digitale identiteit van een eindgebruiker, eindgebruiker devices en ICT-systemen, • Vaststellen van hardware, software en configuratie-technische kenmerken van een netwerktoegang zoekend ICT-systeem, • Samenstellen netwerk toegangspolicies, • Dynamisch opleggen netwerk toegangspolicies,
Services dat het bouwblok biedt (aan de omgeving)	• Beveiliging van interne netwerktoegang, • Beveiliging van externe netwerktoegang.
Kwaliteitskenmerken	Ten behoeve van het faciliteren beveiliging van interne netwerktoegang zijn onderstaande kwaliteitskenmerken van toepassing: • Het bouwblok dient de digitale identiteit van eindgebruikers en van binnen de infrastructuur aanwezige devices en ICT-systemen te kunnen vaststellen tegen de centrale IAM-service van de gemeente. • Het bouwblok dient ondersteuning te bieden aan fallback methoden indien een eindgebruiker device of ICT-systeem de IEEE 802.1X standaard niet ondersteunt (e.g. MAB of WebAuth). • Het bouwblok dient een dermate niveau van granulariteit van toegangspolicies mogelijk te maken opdat voldaan kan worden aan de vigerende richtlijnen op het vlak van informatiebeveiliging van de gemeente. • Het bouwblok dient in ieder geval te voorzien in ondersteuning van binnen de gemeentelijke ICT-infrastructuur gebruikte en onder het beheer-regime van de gemeente vallende typen en modellen eindgebruiker devices en ICT-systemen t.b.v. het samenstellen van dynamische toegangspolicies. Deze policies moeten hardware- en/of software- en/of configuratie-kenmerken van het netwerktoegang zoekende device/ICT-systeem kunnen onderscheiden.

Bouwblok – Centrale Netwerktoegang Verlening	
	• Het bouwblok dient ook in 'monitor' of 'leer' modus te kunnen worden geconfigureerd, opdat het effect van beveiligingspolicies geëvalueerd kunnen, alvorens afgedwongen te worden op access-nodes in een LAN. Ten behoeve van het faciliteren beveiliging van externe netwerktoegang zijn onderstaande kwaliteitskenmerken van toepassing: • Het bouwblok dient de digitale identiteit van eindgebruikers en door de gemeente gebruikte ICT-systemen te kunnen vaststellen tegen de centrale IAM-service van de gemeente. • Het bouwblok dient een dermate niveau van granulariteit van toegangspolicies mogelijk te maken opdat voldaan kan worden aan de vigerende richtlijnen op het vlak van informatiebeveiliging van de gemeente. • Het bouwblok dient in ieder geval te voorzien in ondersteuning van onder het beheer-regime van de gemeente vallende typen en modellen eindgebruiker devices en ICT-systemen t.b.v. het samenstellen van dynamische toegangspolicies. Deze policies moeten hardware- en/of software- en/of configuratie-kenmerken van het netwerktoegang zoekende device/ICT-systeem kunnen onderscheiden. Generieke kwaliteitskenmerken van het bouwblok: • Het bouwblok en haar functies moeten (in termen van capaciteit) geschaald zijn naar de omvang van de afname door eindgebruikers van de gemeente, en flexibiliteit bieden om te voorzien in eventuele krimp en groei in de afname van de te beveiligen toegangsdiensten. • Het platform waaruit de centrale voorziening, die de beveiliging van de netwerktoegang faciliteert, is opgebouwd, dient dusdanig te zijn vormgegeven, dat uitval van één (1) node (i.e. instantie) in dat platform niet mag leiden tot totale uitval van functionaliteit van de voorziening, opdat interne of externe netwerktoegang onmogelijk is. • Het bouwblok dient te voorzien in logging en rapportage-mogelijkheden m.b.t. de beveiliging van netwerktoegang op de access-nodes in een locatie netwerk. • Het bouwblok dient actief gemonitord te worden, opdat de beveiliging van netwerktoegang geborgd kan worden.
Relatie met omgeving	Het bouwblok CNV communiceert: • O.b.v. de IEEE 802.1X standaard voor port-based netwerktoegang en het RADIUS protocol met een access-nodes in de infrastructuur op een gemeentelijke locatie voor het beveiligen van interne netwerktoegang; • O.b.v. het RADIUS protocol met een VPN head-end in het on-premises datacenter voor het beveiligen van externe netwerktoegang (via Internet). Het bouwblok CNV verifieert zowel in geval van interne als van externe netwerktoegang de digitale identiteit van een eindgebruiker,eindgebruiker device en/ of ICT-systeem tegen de centrale directory service (IdP) (van de IAM-omgeving) van de gemeente.

Architectuureis NW-17 - Kenmerken Centrale Netwerktoegang Verlening	
NW-17.1	Zowel gebruikers als (ICT-)systemen dienen eerst te (kunnen) worden geauthentiseerd en geautoriseerd, voordat toegang wordt verleend tot het netwerk van de gemeente.

Architectuureis NW-17 - Kenmerken Centrale Netwerktoegang Verlening	
NW-17.2	De access-node, waaraan een eindgebruiker/ICT-systeem fysiek gekoppeld is, communiceert o.b.v. het IEEE 802.1X protocol met de centrale voorziening, die beveiliging van netwerktoegang faciliteert.
NW-17.3	De centrale voorziening, die de beveiliging van de netwerktoegang faciliteert,voorziet in functionaliteit om o.b.v. real-time verkregen: • hardware, en/of • software, en/of • configuratie kenmerken van het netwerktoegang zoekende ICT-systeem specifieke dynamische beveiligingspolicies toe te passen (e.g. beperkte (i.e. 'quarantaine' of 'gast' toegang) of (least privileged) geautoriseerde toegang).
NW-17.4	De centrale voorziening, die de beveiliging van de netwerktoegang faciliteert, moet als (RADIUS) authenticatie-proxy kunnen functioneren tegen de centrale directory service (IdP) (van de IAM-omgeving) van de gemeente, teneinde user credentials en PKI-certificaten te kunnen verifiëren. Hierbij dienen specifieke kenmerken van de digitale identiteit van een eindgebruiker of (ICT-) systeem binnen de centrale directory service te kunnen worden toegepast bij de samenstelling van de dynamisch af te dwingen beveiligingspolicies door deze centrale voorziening op de netwerknode, die logisch of fysiek toegang verleent tot het netwerk van de gemeente.
NW-17.5	De centrale voorziening, die de beveiliging van de netwerktoegang faciliteert, dient authenticatie methoden te ondersteunen o.b.v. digitale certificaten.
NW-17.6	De centrale voorziening, die de beveiliging van de netwerktoegang faciliteert, dient ook (als fallback mechanisme) dynamische beveiligingspolicies te kunnen opleggen o.b.v.: • een centraal geadministreerde lijst met MAC-adressen van 'vertrouwde' device, en • een web-portaal voor 'gastgebruik'.
NW-17.7	Bij voorkeur voorziet de centrale voorziening, die beveiliging van netwerktoegang faciliteert, in functionaliteit/ondersteuning van protocollen waarmee netwerktoegang (per sessie) wordt verleend o.b.v. digitale kenmerken van zowel een eindgebruiker als het gebruikte ICT-device.
NW-17.8	Het dient mogelijk te zijn een gebruiker of systeem dynamisch te plaatsen in een netwerk segment.
NW-17.9	Het dient mogelijk te zijn een netwerkpoort (van een access-node), waaraan een gebruiker of systeem gekoppeld is, dynamisch te voorzien van een toegangslijst, opdat een gebruiker of systeem beperkt kan worden in de toegestane communicatiemogelijkheden. Deze toegangslijst moet ook in 'monitor' of 'leer' modus toegekend te kunnen worden, opdat het effect ervan geëvalueerd kan worden alvorens dit wordt afgedwongen op data-stromen.
NW-17.10	De centrale voorziening, die de beveiliging van de netwerktoegang faciliteert, dient te voorzien in functionaliteit, die alle drie betrokken aspecten van toegangsbeveiliging ondersteunt: • authenticatie, • autorisatie, • accounting/ logging.
NW-17.11	De centrale voorziening, die de beveiliging van de netwerktoegang faciliteert, dient te voorzien in functionaliteit om (in het kader van auditing) te kunnen rapporteren over de log-informatie m.b.t. netwerktoegang.
NW-17.12	Het platform waaruit de centrale voorziening, die de beveiliging van de netwerktoegang faciliteert, is opgebouwd, dient dusdanig te zijn vormgegeven, dat uitval van één (1) node (i.e. instantie) in dat platform niet mag leiden tot totale uitval van functionaliteit van de voorziening, opdat netwerktoegang onmogelijk is.
NW-17.13	De centrale voorziening, die beveiliging van de netwerktoegang faciliteert, dient te voorzien in een web-based gebruikersinterface waarmee de voorziening functioneel beheerd kan worden.

4.3 Beveiliging van netwerk infrastructuurnodes

Netwerknodes zijn op zichzelf staande entiteiten die beveiligd dienen te worden. Beveiliging op het niveau van de nodes waaruit de netwerk infrastructuur is opgebouwd, houdt onder meer in, dat management planes, control planes en data planes worden beveiligd.
De daadwerkelijk toe te passen beveiligingsmaatregelen op netwerknodes is uiteindelijk gebaseerd op het vigerende beleid op het vlak van informatiebeveiliging.

Architectuureis NW-18 – Beveiliging van netwerknodes	
NW-18.1	Door de markt/industrie als niet-veilig geachte protocollen, technieken of services dienen gedeactiveerd te kunnen worden op netwerknodes.
NW-18.2	Niet-gebruikte services dienen te worden gedeactiveerd op netwerknodes, opdat zo min mogelijk systeemkwetsbaarheden kunnen optreden.
NW-18.3	Niet-gebruikte access en up-/downlink poorten van netwerknodes dienen gedeactiveerd te worden.
NW-18.4	Authenticatie van toegang tot een netwerknode (voor beheerdoeleinden) vindt via een logische of fysieke interface (i.e. via een managementprotocol (e.g. SSHv2) of via de console) plaats o.b.v. het TACACS+ protocol en vindt plaats tegen een centrale IAM-voorziening, waarbij gebruik van lokale settings op een node als fail-safe mechanisme is toegestaan.
NW-18.5	Het beheer van netwerknodes dient te worden uitgevoerd middels managementprotocollen met ingebouwde beveiligingsfuncties (e.g. SSH, HTTPS).
NW-18.6	Autorisatie van toegang tot een netwerknode (voor beheerdoeleinden) vindt plaats o.b.v. het TACACS+ protocol en is gebaseerd op het principe van least privileges ten aanzien van verschillende levels binnen het systeem (RBAC).
NW-18.7	Op het niveau van de management plane dienen passende maatregelen (e.g. rate limiting en anti-spoofing) getroffen te kunnen worden om DoS-aanvallen en man-in-the-middle aanvallen te voorkomen.
NW-18.8	Op het niveau van de control plane dienen passende maatregelen (e.g. rate limiting en anti-spoofing) getroffen te worden om DoS-aanvallen en man-in-the-middle aanvallen te voorkomen.
NW-18.9	Op het niveau van de data plane dienen passende maatregelen (e.g. anti-spoofing) getroffen te worden om DoS-aanvallen en man-in-the-middle aanvallen te voorkomen.

4.4 Netwerkbeheer

Het vanuit één centraal platform kunnen beheren van de netwerkinfrastructuur verhoogt het kwaliteits- en beveiligingsniveau van de netwerkdiensten, die geleverd worden. Door zoveel mogelijk op basis van een *single pane of glass* de netwerkinfrastructuur te kunnen beheren en monitoren kunnen maximale garanties geboden worden op het correct functioneren van de technische netwerknodes.
Het bouwblok *Centrale Netwerk Management Voorziening* (CNMV) levert diensten die dit gecentraliseerde technische beheer op de netwerkinfrastructuur mogelijk maken.

Bouwblok – Centrale Netwerk Management Voorziening	
(Beknopte) Conceptuele beschrijving van het bouwblok	Het bouwblok Centrale Netwerk Management Voorziening voorziet in functionaliteit om netwerknodes in de gemeentelijke ICT-infrastructuur technisch te beheren vanuit één (1) centraal management platform dat toegankelijk is voor beheerders via een web-based portaal. Het bouwblok Centrale Netwerk Management Voorziening is ondergebracht in het on-premises datacenter.
Functies van het bouwblok	• Faciliteren initiële van systeeminrichting,

Bouwblok – Centrale Netwerk Management Voorziening	
	• Registreren/ opslaan van actuele van systeemconfiguratie, • Afdwingen/ opleggen/ herstellen van systeemconfiguraties en -policies, • Toepassen van systeemupdates, • Monitoren van systeemconfiguratie en -policies, • Bieden van inzicht in actuele status van netwerknodes.
Services dat het bouwblok biedt (aan de omgeving)	• Beheer netwerknodes (op basis van automation), • Monitoring netwerknodes.
Kwaliteitskenmerken	*De onderstaande kwaliteitskenmerken zijn van toepassing op het bouwblok:* • Teneinde haar services te bieden aan netwerknodes wordt gebruik gemaakt van in de markt gangbare open standaard protocollen. • Het bouwblok voorziet in een audit-trail op technisch beheer activiteiten m.b.t. functionaliteit van het bouwblok. • Het bouwblok en haar functies moeten (in termen van capaciteit) geschaald zijn naar het aantal technisch te beheren netwerknodes in de ICT-infrastructuur van de gemeente. • Uitval van services van bouwblok Centrale Netwerk Management Voorziening mag geen impact hebben op de operationele status van netwerknodes in de ICT-infrastructuur van de gemeente. • Het platform, waaruit bouwblok Centrale Netwerk Management Voorziening is opgebouwd, dient dusdanig te zijn vormgegeven dat de door dit bouwblok geleverde services beschikbaar blijven bij uitval van één (1) complete on-premises datacenter locatie.
Relatie met omgeving	Het bouwblok dient DC-LAN aansluiting te hebben met access-nodes uit bouwblok Datacenter Netwerk teneinde de services te kunnen bieden aan de netwerknodes uit datzelfde bouwblok Datacenter netwerk. Voor het beveiligen van toegang door technisch beheerders tot het bouwblok wordt er gebruik gemaakt van de centrale directory service (IdP) (van de IAM-omgeving) van de gemeente.

Architectuureis NW-19 – Kenmerken Centraal Netwerkbeheer	
NW-19.1	De centrale netwerk beheervoorziening, waarmee netwerknodes technisch beheerd kunnen worden, dient te voorzien in functionaliteit om netwerknodes en hun actuele systeemconfiguraties te registreren.
NW-19.2	De centrale netwerk beheervoorziening, waarmee netwerknodes technisch beheerd kunnen worden, dient te voorzien in functionaliteit om de (actuele) operationele status van netwerknodes te monitoren. Zowel het actief als passief monitoren van netwerknodes op basis van in de markt gangbare open standaarden (e.g. SNMPv3) moet hierbij mogelijk zijn.
NW-19.3	De centrale netwerk beheervoorziening, waarmee netwerknodes technisch beheerd kunnen worden, dient log-data van netwerknodes o.b.v. in de markt gangbare protocollen (e.g. syslog, CEF) te kunnen ontvangen en opslaan voor nadere analyse.
NW-19.4	De centrale netwerkbeheervoorziening, waarmee netwerknodes technisch beheerd kunnen worden, dient protocollen (e.g. SFlow, NetFlow, IPFIX of gelijkwaardig) te ondersteunen waarmee informatie m.b.t. analyse van het netwerkverkeer verzameld kan worden.

Architectuureis NW-19 – Kenmerken Centraal Netwerkbeheer	
NW-19.5	De centrale netwerk beheervoorziening, waarmee netwerknodes technisch beheerd kunnen worden, dient te voorzien in functionaliteit om op afstand: • netwerknodes te voorzien van softwarematige beveiliging- en systeemupdates, • de technische configuratie van netwerknodes te backuppen, • de technische configuratie van netwerknodes te restoren, • de technische configuratie van netwerknodes af te dwingen (via in de markt gangbare open standaard protocollen (e.g. TLSv1.3, SSHv2, NETCONF, RESTCONF of gelijkwaardig)).
NW-19.6	De centrale netwerkbeheervoorziening, waarmee netwerknodes technisch beheerd kunnen worden, wordt vormgegeven via een fysieke appliance of virtual machine (i.e. VMWare ESXi) appliance.
NW-19.7	De centrale netwerkbeheervoorziening, waarmee netwerknodes technisch beheerd kunnen worden, dient te voorzien in functionaliteit waarmee rapportages kunnen worden verkregen over: • actuele hard- en softwarematige configuraties van netwerknodes, • operationele status van netwerknodes, • historische data over de prestatie van netwerknodes.
NW-19.8	Bij uitval van (functionaliteit van) de centrale netwerk beheervoorziening is er geen impact op het operationele functioneren van netwerknodes in de infrastructuur.
NW-19.9	De centrale netwerkbeheervoorziening, waarmee netwerknodes technisch beheerd kunnen worden, dient te voorzien in een web-based gebruikersinterface waarmee de voorziening functioneel beheerd kan worden. Er geldt dat: • Toegang tot de web-based interface is beveiligd door authenticatie van user credentials van beheerders tegen de centrale directory service (van de IAM-omgeving) van de gemeente. • Autorisatie van beheerders tot functionaliteit gebeurt o.b.v. RBAC (least privileged access). • Audit logs worden bijgehouden van alle beheeractiviteiten.

Bijlage A: Totaaloverzicht architectuureisen domein Netwerk

Netwerkdiensten

Architectuureis NW-01 - Beschikbaarheid netwerkdiensten	
NW-01.1	Bedrade toegang tot het netwerk in een kantoorlocatie heeft een beschikbaarheidseis van 99,8% (tijdens kantooruren).
NW-01.2	Onbedrade toegang tot het netwerk in een kantoorlocatie heeft een beschikbaarheidseis van 99,8% (tijdens kantooruren).
NW-01.3	Bedrade toegang tot het netwerk in een on-premises datacenter locatie heeft een beschikbaarheidseis van 99,9% (24x7).
NW-01.4	Intra-netwerk connectiviteit (binnen een fysieke locatie of via een WAN-connectie tussen fysieke locaties van de gemeente) heeft een beschikbaarheidseis van 99,9% (24x7).
NW-01.5	Extra-netwerk connectiviteit heeft een beschikbaarheidseis van 99,9% (24x7).
NW-01.6	Internet connectiviteit heeft een beschikbaarheidseis van 99,9% (24x7).

Architectuureis NW-02 – Inzet *managed* diensten	
NW-02.1	Internet connectiviteit wordt als *managed* OSI Laag-3 dienst afgenomen van een externe provider. Het fysieke koppelvlak, dat een dergelijke dienst termineert, bevindt zich op een on-premises datacenter locatie.
NW-02.2	Extranet connectiviteit wordt als *managed* OSI laag-3 dienst afgenomen van een externe provider. Het fysieke koppelvlak, dat een dergelijke dienst termineert, bevindt zich op een on-premises datacenter locatie.
NW-02.3	Intranet connectiviteit (tussen twee fysieke locaties van de gemeente) wordt bij voorkeur als een managed OSI laag-2 afgenomen, tenzij: • dit uit het oogpunt van informatieveiligheid onwenselijk is en tot risico's leidt die niet afdoende gemitigeerd kunnen worden; of • dit economisch gezien ongunstig is; of • dit technisch gezien ongewenst is (e.g. omdat het netwerktopologisch kan leiden tot inefficiënt gebruik van netwerkpaden (lees: STP- blokkades)); of • het connectiviteit betreft tussen datacenter locaties; in dit geval wordt connectiviteit o.b.v. *dark fibre* ingezet. Het fysieke koppelvlak dat een dergelijke dienst termineert, bevindt zich (behalve uiteraard een datacenter-interconnect verbinding) op een on-premises datacenter locatie en een decentrale locatie van de gemeente.

Module Datacenter

Architectuureis NW-03 - Generieke kenmerken Datacenter Netwerk	
NW-03.1	Nodes in sub-bouwblok Aggregatie & core laag van het bouwblok Datacenter Netwerk ontsluiten: • zowel de access-nodes van het bouwblok Locatie Netwerk (type Centraal), • als access-nodes van het bouwblok Datacenter Netwerk, • als access nodes uit het bouwblok Edge Netwerk.
NW-03.2	Het toe te passen medium tussen netwerknodes in het bouwblok Edge Netwerk en het bouwblok Datacenter Netwerk (i.e. in sub-bouwblok Aggregatie & core laag) is koper.
NW-03.3	Het toe te passen medium tussen netwerknodes in sub-bouwblok Access laag en sub-bouwblok Aggregatie & core laag van het bouwblok Datacenter Netwerk is koper.
NW-03.4	Het toe te passen medium tussen netwerknodes binnen sub-bouwblok Aggregatie & core laag van bouwblok Datacenter Netwerk is koper.
NW-03.5	De ontsluiting van een netwerknode in sub-bouwblok Aggregatie & core laag naar de access-laag (Locatie Netwerk – type Centraal) bestaat uit minimaal 2x fysieke uplinkconnectie (minimaal 10 Gbit/s per connectie).
NW-03.6	Per netwerknode in sub-bouwblok Aggregatie & core laag is sprake van één logische downlink naar de access laag (Locatie Netwerk – type Centraal). Deze logische downlinkconnectie wordt middels linkbundelingstechnologie vormgegeven.
NW-03.7	De ontsluiting van een netwerknode in sub-bouwblok Aggregatie & core laag naar de access-laag binnen het bouwblok Datacenter Netwerk bestaat uit minimaal 2x fysieke uplink connectie (minimaal 10 Gbit/s per connectie).
NW-03.8	Per netwerknode in sub-bouwblok Aggregatie & core laag is sprake van één logische downlink naar de access- laag van het bouwblok Datacenter Netwerk. Deze logische downlink wordt middels linkbundelingstechnologie vormgegeven.
NW-03.9	De ontsluiting van een netwerknode in het bouwblok Edge Netwerk naar sub-bouwblok Aggregatie & core laag van bouwblok Datacenter Netwerk heeft per fysieke uplinkconnectie minimaal een capaciteit van 10 Gbit/s.
NW-03.10	De capaciteit van de fysieke connectiviteit tussen netwerknodes in sub-bouwblok Aggregatie & core laag van het bouwblok Datacenter Netwerk is minimaal 40 Gbit/s.
NW-03.11	De connectiviteit tussen netwerknodes in sub-bouwblok Aggregatie & core laag van het bouwblok Datacenter Netwerk bestaat uit minimaal 2 fysieke verbindingen.
NW-03.12	OSI-laag 2 netwerkconstructs (e.g. VLAN) dienen beschikbaar gemaakt te kunnen worden 'op' meerdere on-premises datacenter locaties (i.e. 'stretched').
NW-03.13	De beschikbaarheid van de vanuit het Datacenter Netwerk geboden netwerkdiensten is minimaal 99,9%.
NW-03.14	Netwerknodes binnen het bouwblok Datacenter Netwerk dienen virtualisatietechnieken te ondersteunen waarmee logische scheiding van de netwerkinfrastructuur op OSI Laag-2 en OSI Laag-3 niveau te bewerkstelligen is, zodat zonering een end-to-end concept is.
NW-03.15	Netwerknodes binnen het bouwblok Datacenter Netwerk leveren services aan en/of nemen services af uit hun omgeving o.b.v. protocollen die gelden als open standaarden.

Architectuureis NW-04 - Kenmerken access-nodes Datacenter Netwerk	
NW-04.1	Een access-node is redundant verbonden met de ontsluitende/bovenliggende netwerknode(s) binnen sub-bouwblok Aggregatie & core laag.
NW-04.2	Redundantie van uplink/downlinkverbindingen dienen middels linkbundelingstechnologie te kunnen worden vormgegeven.
NW-04.3	De access-poorten van een access-node zijn van het type koper met minimaal de ondersteuning van de interfacesnelheden 1 Gbit/s en 10 Gbit/s.
NW-04.4	Access-nodes hebben 48 access-poorten.
NW-04.5	De uplink/downlinkverbindingen van een access-node naar ontsluitende/bovenliggende node(s) in sub-bouwblok Aggregatie & core laag zijn van het type koper met minimaal de ondersteuning van de interfacesnelheden 10 Gbit/s.

Architectuureis NW-04 - Kenmerken access-nodes Datacenter Netwerk	
NW-04.6	Access-nodes dienen zowel het IPv4- als IPv6-protocol te ondersteunen.
NW-04.7	Access-nodes dienen Quality of Service (QoS) te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
NW-04.8	Access-nodes dienen protocollen te ondersteunen waarmee informatie over aanpalende nodes op het niveau van OSI-laag 1 en 2 kan worden ingewonnen, waarbij het van belang is open standaarden te kunnen gebruiken.
NW-04.9	Access-nodes zijn voorzien van redundante voedingen.
NW-04.10	Access-nodes dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij (conform actuele best practices) echter wel simultaan gebruik- gemaakt kan worden van alle beschikbare netwerkpaden.
NW-04.11	Access-nodes dienen technieken te ondersteunen t.b.v. softwarematige updates waarmee de continuïteit van de door de nodes geboden diensten maximaal wordt gewaarborgd (i.e ISSU, of gelijkwaardige techniek).
NW-04.12	OSI Laag 3 terminatiepunten liggen bij voorkeur op het niveau van de centrale PEP-functionaliteiten, maar in ieder geval binnen het bouwblok Datacenter Netwerk.
NW-04.13	Access-nodes worden bij voorkeur afgenomen van één vendor vanwege: - eenvoud van beheer, - gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), - ter voorkoming van compatibiliteitsissues.
NW-04.14	Access-nodes communiceren met hun omgeving op basis van open standaarden.
NW-04.15	Access-nodes dienen informatie betreffende hun (operationele) werking te kunnen loggen op externe hosts/oplossingen o.b.v. in de markt gangbare methoden en standaarden (e.g. syslog, ReST API, CEF).
NW-04.16	Access-nodes dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van ongeoorloofde koppeling van netwerknodes aan het netwerk (e.g. BPDU guard of gelijkwaardige technieken) (e.g. ter preventie van mac flooding).
NW-04.17	Access-nodes dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van misbruik van toegang tot het netwerk (e.g. dynamic arp protection, DHCP snooping of gelijkwaardige technieken).
NW-04.18	Access-nodes dienen managementprotocollen met ingebouwde beveiligingsfuncties te ondersteunen conform actuele standaarden (e.g. SNMPv3, SSHv2, TLSv1.3). Managementprotocollen zonder ingebouwde beveiligingsfuncties zijn niet toegestaan (e.g. Telnet).
NW-04.19	Access-nodes dienen te beschikken over poorten die geschikt zijn voor het koppelen van netwerkbekabeling middels SFP-gebaseerde modules.
NW-04.20	Access-nodes dienen hun lokale clock te kunnen synchroniseren aan externe referenties/bronnen o.b.v. het NTP-protocol.
NW-04.21	Access-nodes dienen 'name resolution' te kunnen verrichten o.b.v. DNS.
NW-04.22	Access-nodes dienen multicastverkeer te ondersteunen o.b.v. in de markt gangbare en gestandaardiseerde protocollen (e.g. IGMP, PIM).
NW-04.23	Access-nodes dienen het transport van 'jumbo' frames te ondersteunen.
NW-04.24	Access-nodes dienen protocollen of technieken (e.g. SGT of functioneel vergelijkbaar) te ondersteunen waarmee op access-poortniveau beperkingen opgelegd/afgedwongen kunnen worden m.b.t. toegangsrechten tot de netwerkinfrastructuur (opdat micro-segmentatie mogelijk is).
NW-04.25	Access-nodes dienen zowel het RADIUS- als TACACS+ protocol te ondersteunen.
NW-04.26	Access-nodes dienen authenticatie methoden o.b.v. PKI-certificaten te ondersteunen, waarbij uitgifte van deze digitale certificaten via auto-enrollment (i.e. het SCEP protocol) verloopt.
NW-04.27	Access-nodes dienen technieken te ondersteunen waarmee stabiliteit/robuustheid van de control-plane geborgd kan worden (e.g. CoPP of gelijkwaardig).
NW-04.28	Access-nodes dienen de mogelijkheid te bieden om te kunnen worden opgenomen in een software-defined netwerk concept (i.e. 'SDN-ready').

Architectuureis NW-04 - Kenmerken access-nodes Datacenter Netwerk	
NW-04.29	Access-nodes dienen te beschikken over een separaat OOB-interface voor management doeleinden.
NW-04.30	Beheer van access-nodes vindt zoveel mogelijk plaats vanuit/vanaf een centraal management platform. Dit centrale platform levert diensten voor het: • configureren, • monitoren van de operationele status, en • herstellen van functionaliteit (i.e. middels backup en restore), van netwerknodes.
NW-04.31	Het dient mogelijk te zijn om vanaf een centraal management platform technische configuratie op access nodes af te dwingen (via in de markt gangbare open standaard protocollen (e.g. TLSv1.3, SSHv2, NETCONF, RESTCONF of gelijkwaardig)).

Architectuureis NW-05 - Kenmerken netwerknodes Aggregatie & core laag	
NW-05.1	De ontsluiting tussen netwerknodes in sub-bouwblok Aggregatie & core laag onderling moet een capaciteit hebben van 40 Gbit/s.
NW-05.2	Een netwerk node in sub-bouwblok Aggregatie & core laag dient minimaal te voorzien in een combinatie van 1 Gbit/s en 10 Gbit/s poorten.
NW-05.3	Een netwerk node in sub-bouwblok Aggregatie & core laag voorziet in non-oversubscribed poorten (op elke poort).
NW-05.4	Redundantie van uplink/downlinkverbindingen dient middels linkbundelingstechnologie te kunnen worden vormgegeven
NW-05.5	De poorten van een netwerknode in sub-bouwblok Aggregatie & core laag zijn van het type koper met minimaal de ondersteuning van de interfacesnelheden 1 Gbit/s en 10 Gbit/s.
NW-05.6	Een netwerk node in sub-bouwblok Aggregatie & core laag heeft 48 access-poorten en is bij voorkeur modulair uitbreidbaar.
NW-05.7	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen zowel data-transport o.b.v. het IPv4- als IPv6-protocol te ondersteunen.
NW-05.8	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen Quality of Service (QoS) te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
NW-05.9	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen protocollen te ondersteunen waarmee informatie over aanpalende nodes op het niveau van OSI-laag 1 en 2 kan worden ingewonnen, waarbij het van belang is open standaarden te kunnen gebruiken.
NW-05.10	Netwerknodes in sub-bouwblok Aggregatie & core laag zijn voorzien van redundante voedingen.
NW-05.11	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij (conform actuele best practices) echter wel simultaan gebruikgemaakt kan worden van alle beschikbare netwerkpaden.
NW-05.12	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen technieken te ondersteunen t.b.v. softwarematige updates waarmee continuïteit van de door de nodes geboden diensten maximaal wordt gewaarborgd (i.e ISSU, of gelijkwaardige techniek).
NW-05.13	OSI Laag 3 terminatiepunten liggen bij voorkeur op het niveau van de centrale PEP-functionaliteiten, maar in ieder geval binnen bouwblok Datacenter Netwerk.
NW-05.14	Netwerknodes in sub-bouwblok Aggregatie & core laag worden bij voorkeur afgenomen van één vendor vanwege: - eenvoud van beheer, - gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), ter voorkoming van compatibiliteitsissues.
NW-05.15	Netwerknodes in sub-bouwblok Aggregatie & core laag communiceren met hun omgeving op basis van open standaarden.

Architectuureis NW-05 - Kenmerken netwerknodes Aggregatie & core laag	
NW-05.16	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen informatie betreffende hun (operationele) werking te kunnen loggen op externe hosts/oplossingen o.b.v. in de markt gangbare methoden en standaarden (e.g. syslog, ReST API, CEF).
NW-05.17	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen protocollen te ondersteunen waarmee analyse van het netwerkverkeer mogelijk is (e.g. SPAN of gelijkwaardig).
NW-05.18	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen protocollen te ondersteunen waarmee statistische analyse van het netwerkverkeer mogelijk is (e.g. sFlow, NetFlow, IPFIX of gelijkwaardig).
NW-05.19	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van ongeoorloofde koppeling van nodes aan het netwerk (e.g. BPDU guard of gelijkwaardige technieken).
NW-05.20	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van misbruik van toegang tot het netwerk (e.g. dynamic arp protection, DHCP snooping of gelijkwaardige technieken).
NW-05.21	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen managementprotocollen met ingebouwde beveiligingsfuncties te ondersteunen conform actuele standaarden (e.g. SNMPv3, SSHv2, TLSv1.3). Managementprotocollen zonder ingebouwde beveiligingsfuncties zijn niet toegestaan (e.g. Telnet).
NW-05.22	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen te beschikken over poorten die geschikt zijn voor het koppelen van netwerkbekabeling middels SFP-gebaseerde modules.
NW-05.23	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen hun lokale clock te kunnen synchroniseren aan externe referenties/ bronnen o.b.v. het NTP-protocol.
NW-05.24	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen 'name resolution' te kunnen verrichten o.b.v. DNS.
NW-05.25	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen multicast verkeer te ondersteunen o.b.v. in de markt gangbare protocollen (e.g. IGMP, PIM).
NW-05.26	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen in de markt gangbare protocollen te ondersteunen waarmee een netwerknode de 'next hop' bepaalt voor een netwerkpakket, indien een virtuele node (e.g. virtuele router) de next hop is voor het netwerkverkeer (e.g. VRRP).
NW-05.27	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen transport van 'jumbo' frames te ondersteunen.
NW-05.28	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen protocollen of technieken (e.g. SGT, SXP of functioneel vergelijkbaar) te ondersteunen waarmee op access-poort niveau beperkingen opgelegd/ afgedwongen kunnen worden m.b.t. toegangsrechten tot de netwerkinfrastructuur (opdat micro-segmentatie/host-isolation mogelijk is).
NW-05.29	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen zowel het RADIUS- als TACACS+ protocol te ondersteunen.
NW-05.30	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen authenticatie methoden o.b.v. PKI-certificaten te ondersteunen, waarbij uitgifte van deze digitale certificaten via auto-enrollment (i.e. het SCEP protocol) verloopt.
NW-05.31	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen technieken te ondersteunen waarmee stabiliteit/robuustheid van de control-plane geborgd kan worden (e.g. CoPP of gelijkwaardig).
NW-05.32	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen de mogelijkheid te bieden om te kunnen worden opgenomen in een software-defined netwerk concept (i.e. 'SDN-ready').
NW-05.33	Netwerknodes in sub-bouwblok Aggregatie & core laag dienen te beschikken over een separaat OOB-interface voor management doeleinden.
NW-05.34	Beheer van netwerknodes in sub-bouwblok Aggregatie & core laag vindt zoveel mogelijk plaats vanuit vanaf een centraal management platform. Dit centrale platform levert diensten voor het: • configureren, • monitoren van de operationele status, en • herstellen van functionaliteit (i.e. middels backup en restore),

Architectuureis NW-05 - Kenmerken netwerknodes Aggregatie & core laag	
	van netwerknodes.
NW-05.35	Het dient mogelijk te zijn om vanaf een centraal management platform technische configuratie op netwerknodes in sub-bouwblok Aggregatie & core laag af te dwingen (via in de markt gangbare open standaard protocollen (e.g. TLSv1.3, SSHv2, NETCONF, RESTCONF of gelijkwaardig)).

Module Edge

Architectuureis NW-06 - Generieke kenmerken Edge Netwerk	
NW-06.1	Het bouwblok Edge Netwerk bestaat louter uit access-nodes. Deze nodes zijn fysiek ondergebracht in de on-premises datacenter locaties van de gemeente.
NW-06.2	Nodes in de access-laag van het bouwblok Edge Netwerk ontsluiten: • netwerknodes (e.g. routers) die op een on-premises datacenter locatie het fysieke koppelvlak vormen voor ofwel INTRA-netwerk (i.e. WAN) ofwel EXTRA-netwerk ofwel INTERNET connectiviteitsdiensten; en deze access-nodes van bouwblok Edge Netwerk worden zelf ontsloten naar: • netwerknodes in sub-bouwblok Aggregatie & core laag van bouwblok Datacenter Netwerk.
NW-06.3	Ontsluiting van een netwerknode in de access-laag van het bouwblok Edge Netwerk naar de netwerknodes in sub-bouwblok Aggregatie & core laag van bouwblok Datacenter Netwerk) bestaat uit minimaal 2x fysieke uplink- connecties o.b.v. koper (minimaal 10 Gbit/s per connectie).
NW-06.4	Per netwerknode in de accesslaag van bouwblok Edge Netwerk is sprake van één logische uplink naar een netwerknodes in sub-bouwblok Aggregatie & core laag (Datacenter Netwerk). Deze logische uplink wordt middels linkbundelingstechnologie vormgegeven.
NW-06.5	De beschikbaarheid van de vanuit het Edge Netwerk geboden netwerkdiensten is minimaal 99,9%.
NW-06.6	Netwerknodes binnen het bouwblok Edge Netwerk dienen virtualisatietechnieken te ondersteunen waarmee logische scheiding van de netwerkinfrastructuur op OSI Laag-2 en OSI Laag-3 niveau te bewerkstelligen is, zodat zonering een end-to-end concept is.
NW-06.7	Netwerknodes binnen het bouwblok Edge Netwerk leveren services aan en/ of nemen services af uit hun omgeving o.b.v. protocollen die gelden als open standaarden.

Architectuureis NW-07 - Kenmerken access-nodes Edge Netwerk	
NW-07.1	Een access-node is redundant verbonden met de ontsluitende/bovenliggende node(s) binnen sub-bouwblok Aggregatie & core laag van het bouwblok Datacenter Netwerk.
NW-07.2	Redundantie van uplink/downlinkverbindingen dient middels linkbundelingstechnologie te kunnen worden vormgegeven
NW-07.3	De access-poorten van een access-node zijn van het type koper of glas met minimaal de ondersteuning van de interfacesnelheden 1 Gbit/s en 10 Gbit/s.
NW-07.4	Access-nodes hebben 48 access-poorten.
NW-07.5	De uplink/downlinkverbindingen van een access-node naar ontsluitende/bovenliggende node(s) in sub-bouwblok Aggregatie & core laag van het bouwblok Datacenter Netwerk zijn van het type koper met minimaal de ondersteuning van de interfacesnelheden 10 Gbit/s.
NW-07.6	Access-nodes dienen zowel datatransport o.b.v. het IPv4- als IPv6-protocol te ondersteunen.
NW-07.7	Access-nodes dienen Quality of Service (QoS) te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
NW-07.8	Access-nodes dienen protocollen te ondersteunen waarmee informatie over aanpalende nodes op het niveau van OSI-laag 1 en 2 kan worden ingewonnen, waarbij het van belang is open standaarden te kunnen gebruiken.
NW-07.9	Access-nodes zijn voorzien van redundante voedingen.
NW-07.10	Access-nodes dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij (conform actuele best practices) echter wel simultaan gebruik- gemaakt kan worden van alle beschikbare netwerkpaden.
NW-07.11	Access-nodes dienen technieken te ondersteunen t.b.v. softwarematige updates waarmee continuïteit van de door de nodes geboden diensten maximaal wordt gewaarborgd (i.e ISSU, of gelijkwaardige techniek).
NW-07.12	OSI Laag 3 terminatiepunten liggen bij voorkeur op het niveau van de centrale PEP-functionaliteiten, maar in ieder geval binnen bouwblok Datacenter Netwerk.

Architectuureis NW-07 - Kenmerken access-nodes Edge Netwerk	
NW-07.13	Access-nodes worden bij voorkeur afgenomen van één vendor vanwege: - eenvoud van beheer, - gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), ter voorkoming van compatibiliteitsissues.
NW-07.14	Access-nodes communiceren met hun omgeving op basis van open standaarden.
NW-07.15	Access-nodes dienen informatie betreffende hun (operationele) werking te kunnen loggen op externe hosts/oplossingen o.b.v. in de markt gangbare methoden en standaarden (e.g. syslog, ReST API, CEF).
NW-07.16	Access-nodes dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van ongeoorloofde koppeling van netwerknodes aan het netwerk (e.g. BPDU guard of gelijkwaardige technieken) (e.g. ter preventie van MAC flooding).
NW-07.17	Access-nodes dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van misbruik van toegang tot het netwerk (e.g. dynamic arp protection, DHCP snooping of gelijkwaardige technieken).
NW-07.18	Access-nodes dienen managementprotocollen met ingebouwde beveiligingsfuncties te ondersteunen conform actuele standaarden (e.g. SNMPv3, SSHv2, TLS)v1.3. Managementprotocollen zonder ingebouwde beveiligingsfuncties zijn niet toegestaan (e.g. Telnet).
NW-07.19	Access-nodes dienen te beschikken over poorten die geschikt zijn voor het koppelen van netwerkbekabeling middels SFP-gebaseerde modules.
NW-07.20	Access-nodes dienen hun lokale clock te kunnen synchroniseren aan externe referenties/bronnen o.b.v. het NTP-protocol.
NW-07.21	Access-nodes dienen 'name resolution' te kunnen verrichten o.b.v. DNS.
NW-07.22	Access-nodes dienen multicastverkeer te ondersteunen o.b.v. in de markt gangbare en gestandaardiseerde protocollen (e.g. IGMP, PIM).
NW-07.23	Access-nodes dienen het transport van 'jumbo' frames te ondersteunen.
NW-07.24	Access-nodes dienen protocollen of technieken (e.g. SGT of functioneel vergelijkbaar) te ondersteunen waarmee op access-poort niveau beperkingen opgelegd/afgedwongen kunnen worden m.b.t. toegangsrechten tot de netwerkinfrastructuur (opdat micro-segmentatie mogelijk is).
NW-07.25	Access-nodes dienen zowel het RADIUS- als TACACS+ protocol te ondersteunen.
NW-07.26	Access-nodes dienen authenticatie methoden o.b.v. PKI-certificaten te ondersteunen, waarbij uitgifte van deze digitale certificaten via auto-enrollment (i.e. het SCEP protocol) verloopt.
NW-07.27	Access-nodes dienen technieken te ondersteunen waarmee stabiliteit of robuustheid van de control-plane geborgd kan worden (e.g. CoPP of gelijkwaardig).
NW-07.28	Access-nodes dienen de mogelijkheid te bieden om te kunnen worden opgenomen in een software-defined netwerk concept (i.e. 'SDN-ready').
NW-07.29	Access-nodes dienen te beschikken over een separate OOB-interface voor managementdoeleinden.
NW-07.30	Het beheer van access-nodes vindt zoveel mogelijk plaats vanuit/vanaf een centraal management platform. Dit centrale platform levert diensten voor het: • configureren, • monitoren van de operationele status, en • herstellen van functionaliteit (i.e. middels backup en restore), van netwerknodes.
NW-07.31	Het dient mogelijk te zijn om vanaf een centraal management platform technische configuratie op access nodes af te dwingen (via in de markt gangbare open standaard protocollen (e.g. TLSv1.3, SSHv2, NETCONF, RESTCONF of gelijkwaardig)).

Module Locatie

Architectuureis NW-08 - Generieke kenmerken Locatie Netwerk [type Centraal]	
NW-08.1	Het toe te passen medium tussen netwerknodes in de bouwblokken Locatie Netwerk (i.e. accesslaag van type Centraal) en Datacenter Netwerk (i.e. sub-bouwblok Aggregatie & core laag van het DC-LAN) is koper.
NW-08.2	Ontsluiting van een netwerknode in de access laag (Locatie Netwerk – type Centraal) naar sub-bouwblok Aggregatie & core laag van bouwblok Datacenter Netwerk bestaat uit minimaal 2x fysieke uplink.
NW-08.3	Per netwerk node in de access laag (Locatie Netwerk – type Centraal) is sprake van één logische uplink naar sub-bouwblok Aggregatie & core laag van bouwblok Datacenter Netwerk. Deze logische uplink wordt middels linkbundelingstechnologie vormgegeven.
NW-08.4	Netwerknodes binnen het bouwblok Locatie Netwerk [type Centraal] dienen virtualisatie-technieken te ondersteunen waarmee logische scheiding van de netwerkinfrastructuur op OSI Laag-2 en OSI Laag-3 niveau te bewerkstelligen is, zodat zonering een end-to-end concept is.
NW-08.5	Access nodes leveren services aan en/ of nemen services af uit hun omgeving o.b.v. protocollen die gelden als open standaarden.

Architectuureis NW-09 - Kenmerken access-nodes Locatie Netwerk [type Centraal]	
NW-09.1	Een access-node is redundant verbonden met de ontsluitende/bovenliggende node(s) binnen sub-bouwblok Aggregatie & core laag van bouwblok Datacenter Netwerk.
NW-09.2	Redundantie van uplink/downlinkverbindingen dient middels linkbundelingstechnologie te kunnen worden vormgegeven.
NW-09.3	Uplink/downlinkverbindingen hebben minimaal een capaciteit van 2x 10 Gbit/s.
NW-09.4	De access-poorten van access-nodes zijn van het type koper 10/100/1000 Mbit/s.
NW-09.5	Access-nodes hebben 48 access-poorten.
NW-09.6	Access-nodes dienen te voorzien in Power-over-Ethernet mogelijkheden (o.b.v. de IEEE 802.3at-2009 (PoE+) of een recentere IEEE standaard) om gekoppelde devices (e.g. wireless access points of IP-telefoons) van stroom te kunnen voorzien.
NW-09.7	Access-nodes dienen zowel het IPv4- als IPv6-protocol te ondersteunen.
NW-09.8	Access-nodes dienen Quality of Service (QoS) te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
NW-09.9	Access-nodes dienen protocollen te ondersteunen waarmee informatie over aanpalende nodes op het niveau van OSI-laag 1 en 2 kan worden ingewonnen, waarbij het van belang is open standaarden te kunnen gebruiken.
NW-09.10	Access-nodes zijn voorzien van redundante voedingen.
NW-09.11	Access-nodes dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij (conform actuele best practices) echter wel simultaan gebruik- gemaakt kan worden van alle beschikbare netwerkpaden.
NW-09.12	OSI Laag 3 terminatiepunten liggen bij voorkeur op het niveau van sub-bouwblok Aggregatie & core laag van bouwblok Datacenter Netwerk.
NW-09.13	Access-nodes worden bij voorkeur afgenomen van één vendor vanwege: - eenvoud van beheer, - gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), - ter voorkoming van compatibiliteitsissues.
NW-09.14	Access-nodes communiceren met hun omgeving op basis van open standaarden.
NW-09.15	Access-nodes dienen informatie betreffende hun (operationele) werking te kunnen loggen op externe hosts/ oplossingen o.b.v. in de markt gangbare methoden en standaarden (e.g. syslog, ReST API, CEF).
NW-09.16	Access-nodes dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van ongeoorloofde koppeling van netwerknodes aan het netwerk (e.g. BPDU guard of gelijkwaardige technieken) (e.g. ter preventie van mac flooding).

Architectuureis NW-09 - Kenmerken access-nodes Locatie Netwerk [type Centraal]	
NW-09.17	Access-nodes dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van misbruik van toegang tot het netwerk (e.g. dynamic arp protection, DHCP snooping of gelijkwaardige technieken).
NW-09.18	Access-nodes dienen managementprotocollen met ingebouwde beveiligingsfuncties te ondersteunen conform actuele standaarden (e.g. SNMPv3, SSHv2, TLSv1.3). Managementprotocollen zonder ingebouwde beveiligingsfuncties zijn niet toegestaan (e.g. Telnet).
NW-09.19	Access-nodes dienen technieken te ondersteunen t.b.v. softwarematige updates waarmee continuïteit van de door de nodes geboden diensten maximaal wordt gewaarborgd (i.e ISSU, of gelijkwaardige techniek).
NW-09.20	Access-nodes dienen te beschikken over poorten die geschikt zijn voor het koppelen van netwerkbekabeling middels SFP-gebaseerde modules
NW-09.21	Access-nodes dienen hun lokale clock te kunnen synchroniseren aan externe referenties/bronnen o.b.v. het NTP-protocol.
NW-09.22	Access-nodes dienen 'name resolution' te kunnen verrichten o.b.v. DNS.
NW-09.23	Access-nodes dienen multicastverkeer te ondersteunen o.b.v. in de markt gangbare protocollen (e.g. IGMP, PIM).
NW-09.24	Access-nodes dienen het transport van 'jumbo' frames te ondersteunen.
NW-09.25	Access-nodes dienen (op basis van de IEEE 802.1X standaard) te voorzien in functionaliteit om op access poortniveau dynamisch authenticatie en autorisatie van eindgebruikers en ICT-devices te faciliteren.
NW-09.26	Access-nodes dienen zowel het RADIUS- als TACACS+ protocol te ondersteunen.
NW-09.27	Access-nodes dienen authenticatie methoden o.b.v. PKI-certificaten te ondersteunen, waarbij uitgifte van deze digitale certificaten via auto-enrollment (i.e. het SCEP protocol) verloopt.
NW-09.28	Access-nodes dienen technieken te ondersteunen waarmee stabiliteit of robuustheid van de control-plane geborgd kan worden (e.g. CoPP of gelijkwaardig).
NW-09.29	Access-nodes dienen de mogelijkheid te bieden om te kunnen worden opgenomen in een software-defined netwerk concept (i.e. 'SDN-ready').
NW-09.30	Access-nodes dienen te beschikken over een separate OOB-interface voor management-doeleinden.
NW-09.31	Het beheer van access-nodes vindt zoveel mogelijk plaats vanuit/vanaf een centraal management platform. Dit centrale platform levert diensten voor het • configureren, • monitoren van de operationele status, en • herstellen van functionaliteit (i.e. middels backup en restore), van netwerknodes.
NW-09.32	Het dient mogelijk te zijn om vanaf een centraal management platform technische configuratie op access nodes af te dwingen (via in de markt gangbare open standaard protocollen (e.g. TLSv1.3, SSHv2, NETCONF, RESTCONF of gelijkwaardig)).

Architectuureis NW-10 - Generieke kenmerken Locatie Netwerk [type Decentraal]	
NW-10.1	Het toe te passen medium tussen een access-nodes in het bouwblok Locatie Netwerk (type Decentraal) en een netwerknode, die het fysieke koppelvlak met de INTRA-netwerk (i.e WAN) connectiviteitsdienst vormt, is koper.
NW-10.2	De ontsluiting van een netwerknode in de access laag (Locatie Netwerk – type Decentraal) naar een netwerknode, die het fysieke koppelvlak met de INTRA-netwerk (i.e WAN) connectiviteitsdienst vormt, bestaat (indien mogelijk) uit minimaal 2x fysieke uplink. Alleen de eigenschappen (e.g. geen ondersteuning van linkbundeling of gebrek aan fysieke uplinkpoorten) van de aan een access-node te koppelen netwerknode mogen hierin beperkend zijn.
NW-10.3	Per access node is (indien mogelijk) sprake van één logische uplink naar een netwerknode, die het fysieke koppelvlak met de INTRA-netwerk (i.e WAN) connectiviteitsdienst vormt. Deze logische uplink wordt middels linkbundelingstechnologie vormgegeven.

NW-10.4	Access-nodes binnen het bouwblok Locatie Netwerk [type Decentraal] dienen virtualisatie-technieken te ondersteunen waarmee logische scheiding van de netwerkinfrastructuur op OSI Laag-2 en OSI Laag-3 niveau te bewerkstelligen is, zodat zonering een end-to-end concept is.
NW-10.5	Access-nodes leveren services aan en/ of nemen services af uit hun omgeving o.b.v. protocollen die gelden als open standaarden.

Architectuureis NW-11 - Kenmerken access-nodes Locatie Netwerk [type Decentraal]	
NW-11.1	Een access-node is redundant verbonden met de ontsluitende/bovenliggende node(s).
NW-11.2	Redundantie van uplink/downlinkverbindingen dient middels linkbundelingstechnologie te kunnen worden vormgegeven.
NW-11.3	Uplink/downlinkverbindingen hebben minimaal een capaciteit van 1 Gbit/s.
NW-11.4	De access-poorten van access-nodes zijn van het type koper 10/100/1000 Mbit/s.
NW-11.5	Access-nodes hebben 48 access-poorten.
NW-11.6	Access-nodes dienen te voorzien in Power-over-Ethernet mogelijkheden (o.b.v. de IEEE 802.3at-2009 (PoE+) of een recentere IEEE standaard) om gekoppelde devices (e.g. wireless access points of IP-telefoons) van stroom te kunnen voorzien.
NW-11.7	Access-nodes dienen zowel data-transport o.b.v. het IPv4- als IPv6-protocol te ondersteunen.
NW-11.8	Access-nodes dienen Quality of Service (QoS) te ondersteunen, zowel QoS op het niveau van OSI-laag 2 als OSI-laag 3.
NW-11.9	Access-nodes dienen protocollen te ondersteunen waarmee informatie over aanpalende nodes op het niveau van OSI-laag 1 en 2 kan worden ingewonnen, waarbij het van belang is open standaarden te kunnen gebruiken.
NW-11.10	Access-nodes zijn voorzien van redundante voedingen.
NW-11.11	Access-nodes dienen te voorzien in protocollen waarmee potentiële loops in het netwerk kunnen worden voorkomen, waarbij (conform actuele best practices) echter wel simultaan gebruik- gemaakt kan worden van alle beschikbare netwerkpaden.
NW-11.12	Access-nodes worden bij voorkeur afgenomen van één vendor vanwege: - eenvoud van beheer, - gegarandeerde leverancierssupport voor beheer en technologische doorontwikkelingen van het product (product roadmap), - ter voorkoming van compatibiliteitsissues.
NW-11.13	Access-nodes communiceren met hun omgeving op basis van open standaarden.
NW-11.14	Access-nodes dienen informatie betreffende hun (operationele) werking te kunnen loggen op externe hosts/oplossingen o.b.v. in de markt gangbare methoden en standaarden (e.g. syslog, ReST API, CEF).
NW-11.15	Access-nodes dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van ongeoorloofde koppeling van netwerknodes aan het netwerk (e.g. BPDU guard of gelijkwaardige technieken) (e.g. ter preventie van MAC flooding).
NW-11.16	Access-nodes dienen te kunnen voorzien in beveiligingsmechanismen ter voorkoming van misbruik van toegang tot het netwerk (e.g. dynamic arp protection, DHCP snooping of gelijkwaardige technieken).
NW-11.17	Access-nodes dienen managementprotocollen met ingebouwde beveiligingsfuncties te ondersteunen conform actuele standaarden (e.g. SNMPv3, SSHv2, TLSv1.3). Managementprotocollen zonder ingebouwde beveiligingsfuncties zijn niet toegestaan (e.g. Telnet).
NW-11.18	Access-nodes dienen technieken te ondersteunen t.b.v. softwarematige updates waarmee continuïteit van de door de nodes geboden diensten maximaal wordt gewaarborgd (i.e ISSU, of gelijkwaardige techniek).
NW-11.19	Access-nodes dienen te beschikken over poorten die geschikt zijn voor het koppelen van netwerkbekabeling middels SFP-gebaseerde modules
NW-11.20	Access-nodes dienen hun lokale clock te kunnen synchroniseren aan externe referenties/bronnen o.b.v. het NTP-protocol.
NW-11.21	Access-nodes dienen 'name resolution' te kunnen verrichten o.b.v. DNS.

Architectuureis NW-11 - Kenmerken access-nodes Locatie Netwerk [type Decentraal]	
NW-11.22	Access-nodes dienen multicastverkeer te ondersteunen o.b.v. in de markt gangbare protocollen (e.g. IGMP, PIM).
NW-11.23	Access-nodes dienen het transport van 'jumbo' frames te ondersteunen.
NW-11.24	Access-nodes dienen (op basis van de IEEE 802.1X standaard) te voorzien in functionaliteit om op access poortniveau dynamisch authenticatie en autorisatie van eindgebruikers en ICT-devices te faciliteren.
NW-11.25	Access-nodes dienen zowel het RADIUS- als TACACS+ protocol te ondersteunen.
NW-11.26	Access-nodes dienen authenticatie methoden o.b.v. PKI-certificaten te ondersteunen, waarbij uitgifte van deze digitale certificaten via auto-enrollment (i.e. het SCEP protocol) verloopt.
NW-11.27	Access-nodes dienen technieken te ondersteunen waarmee stabiliteit/ robuustheid van de control-plane geborgd kan worden (e.g. CoPP of gelijkwaardig).
NW-11.28	Access-nodes dienen de mogelijkheid te bieden om te kunnen worden opgenomen in een software-defined netwerk concept (i.e. 'sdn-ready').
NW-11.29	Access-nodes dienen te beschikken over een separate OOB-interface voor management doeleinden.
NW-11.30	Beheer van access-nodes vindt zoveel mogelijk plaats vanuit/ vanaf een centraal management platform. Dit centrale platform levert diensten voor het: • configureren, • monitoren van de operationele status, en • herstellen van functionaliteit (i.e. middels backup en restore), van netwerknodes.
NW-11.31	Het dient mogelijk te zijn om vanaf een centraal management platform technische configuratie op access nodes af te dwingen (via in de markt gangbare open standaard protocollen (e.g. TLSv1.3, SSHv2, NETCONF, RESTCONF of gelijkwaardig)).

Architectuureis NW-12 – Kenmerken Draadloos Locatie Netwerk	
NW-12.1	[Placeholder.]

Beveiliging Netwerk

Architectuureis NW-13 - Gebruik van veilige bekabeling voor data-communicatie	
NW-13.1	Netwerkbekabeling dient te voldoen aan actuele ANSI/TIA en/ of ISO/IEC standaarden (e.g. TIA 568, ISO 11801).

Architectuureis NW-14 - Inzet van betrouwbare middelen	
NW-14.1	Netwerknodes in de ICT-infrastructuur dienen actieve ondersteuning te hebben van de leverancier (i.e. OEM) op de hard- en software, waaruit deze nodes zijn opgebouwd. Technische kwetsbaarheden, die de veilige werking van netwerknodes bedreigen, kunnen zo tijdig gemitigeerd worden. Netwerknodes worden vervangen voordat de actieve ondersteuning vervalt.

Architectuureis NW-15 - Versleuteling van datastromen over externe netwerken	
NW-15.1	Datacommunicatie tussen: • een ICT-device binnen een ICT-infrastructuur (die onder het beheerregime valt) van de gemeente en een ICT-device buiten deze infrastructuur, of • twee ICT-devices binnen delen van ICT-infrastructuren (die onder het beheerregime vallen) van de gemeente en dat deels over een extern (i.e. buiten dit beheerregime vallend) netwerk verloopt, wordt te allen tijde versleuteld o.b.v. in de markt veilig geachte open protocollen (e.g. MACsec of IPSEC).

Architectuureis NW-16 - Afdwingen beveiligingspolicies op data-stromen	
NW-16.1	[Placeholder.]

Architectuureis NW-17 - Kenmerken Centrale Netwerktoegang Verlening	
NW-17.1	Zowel gebruikers als (ICT-)systemen dienen eerst te (kunnen) worden geauthentiseerd en geautoriseerd, voordat toegang wordt verleend tot het netwerk van de gemeente.
NW-17.2	De access-node, waaraan een eindgebruiker/ICT-systeem fysiek gekoppeld is, communiceert o.b.v. het IEEE 802.1X protocol met de centrale voorziening, die beveiliging van netwerktoegang faciliteert.
NW-17.3	De centrale voorziening, die de beveiliging van de netwerktoegang faciliteert,voorziet in functionaliteit om o.b.v. real-time verkregen: • hardware, en/of • software, en/of • configuratie kenmerken van het netwerktoegang zoekende ICT-systeem specifieke dynamische beveiligingspolicies toe te passen (e.g. beperkte (i.e. 'quarantaine' of 'gast' toegang) of (least privileged) geautoriseerde toegang).
NW-17.4	De centrale voorziening, die de beveiliging van de netwerktoegang faciliteert, moet als (RADIUS) authenticatie-proxy kunnen functioneren tegen de centrale directory service (IdP) (van de IAM-omgeving) van de gemeente, teneinde user credentials en PKI-certificaten te kunnen verifiëren.

Architectuureis NW-17 - Kenmerken Centrale Netwerktoegang Verlening	
	Hierbij dienen specifieke kenmerken van de digitale identiteit van een eindgebruiker of (ICT-) systeem binnen de centrale directory service te kunnen worden toegepast bij de samenstelling van de dynamisch af te dwingen beveiligingspolicies door deze centrale voorziening op de netwerknode, die logisch of fysiek toegang verleent tot het netwerk van de gemeente.
NW-17.5	De centrale voorziening, die de beveiliging van de netwerktoegang faciliteert, dient authenticatie methoden te ondersteunen o.b.v. digitale certificaten.
NW-17.6	De centrale voorziening, die de beveiliging van de netwerktoegang faciliteert, dient ook (als fallback mechanisme) dynamische beveiligingspolicies te kunnen opleggen o.b.v.: • een centraal geadministreerde lijst met MAC-adressen van 'vertrouwde' device, en • een web-portaal voor 'gastgebruik'.
NW-17.7	Bij voorkeur voorziet de centrale voorziening, die beveiliging van netwerktoegang faciliteert, in functionaliteit/ondersteuning van protocollen waarmee netwerktoegang (per sessie) wordt verleend o.b.v. digitale kenmerken van zowel een eindgebruiker als het gebruikte ICT-device.
NW-17.8	Het dient mogelijk te zijn een gebruiker of systeem dynamisch te plaatsen in een netwerk segment.
NW-17.9	Het dient mogelijk te zijn een netwerkpoort (van een access-node), waaraan een gebruiker of systeem gekoppeld is, dynamisch te voorzien van een toegangslijst, opdat een gebruiker of systeem beperkt kan worden in de toegestane communicatiemogelijkheden. Deze toegangslijst moet ook in 'monitor' of 'leer' modus toegekend te kunnen worden, opdat het effect ervan geëvalueerd kan worden alvorens dit wordt afgedwongen op data-stromen.
NW-17.10	De centrale voorziening, die de beveiliging van de netwerktoegang faciliteert, dient te voorzien in functionaliteit, die alle drie betrokken aspecten van toegangsbeveiliging ondersteunt: • authenticatie, • autorisatie, • accounting/ logging.
NW-17.11	De centrale voorziening, die de beveiliging van de netwerktoegang faciliteert, dient te voorzien in functionaliteit om (in het kader van auditing) te kunnen rapporteren over de log-informatie m.b.t. netwerktoegang.
NW-17.12	Het platform waaruit de centrale voorziening, die de beveiliging van de netwerktoegang faciliteert, is opgebouwd, dient dusdanig te zijn vormgegeven, dat uitval van één (1) node (i.e. instantie) in dat platform niet mag leiden tot totale uitval van functionaliteit van de voorziening, opdat netwerktoegang onmogelijk is.
NW-17.13	De centrale voorziening, die beveiliging van de netwerktoegang faciliteert, dient te voorzien in een web-based gebruikersinterface waarmee de voorziening functioneel beheerd kan worden.

Architectuureis NW-18 – Beveiliging van netwerknodes	
NW-18.1	Door de markt/industrie als niet-veilig geachte protocollen, technieken of services dienen gedeactiveerd te kunnen worden op netwerknodes.
NW-18.2	Niet-gebruikte services dienen te worden gedeactiveerd op netwerknodes, opdat zo min mogelijk systeemkwetsbaarheden kunnen optreden.
NW-18.3	Niet-gebruikte access en up-/downlink poorten van netwerknodes dienen gedeactiveerd te worden.
NW-18.4	Authenticatie van toegang tot een netwerknode (voor beheerdoeleinden) vindt via een logische of fysieke interface (i.e. via een managementprotocol (e.g. SSHv2) of via de console) plaats o.b.v. het TACACS+ protocol en vindt plaats tegen een centrale IAM-voorziening, waarbij gebruik van lokale settings op een node als fail-safe mechanisme is toegestaan.
NW-18.5	Het beheer van netwerknodes dient te worden uitgevoerd middels managementprotocollen met ingebouwde beveiligingsfuncties (e.g. SSH, HTTPS).
NW-18.6	Autorisatie van toegang tot een netwerknode (voor beheerdoeleinden) vindt plaats o.b.v. het TACACS+ protocol en is gebaseerd op het principe van least privileges ten aanzien van verschillende levels binnen het systeem (RBAC).

Architectuureis NW-18 – Beveiliging van netwerknodes	
NW-18.7	Op het niveau van de management plane dienen passende maatregelen (e.g. rate limiting en anti-spoofing) getroffen te kunnen worden om DoS-aanvallen en man-in-the-middle aanvallen te voorkomen.
NW-18.8	Op het niveau van de control plane dienen passende maatregelen (e.g. rate limiting en anti-spoofing) getroffen te worden om DoS-aanvallen en man-in-the-middle aanvallen te voorkomen.
NW-18.9	Op het niveau van de data plane dienen passende maatregelen (e.g. anti-spoofing) getroffen te worden om DoS-aanvallen en man-in-the-middle aanvallen te voorkomen.

Netwerkbeheer

Architectuureis NW-19 – Kenmerken Centraal Netwerkbeheer	
NW-19.1	De centrale netwerk beheervoorziening, waarmee netwerknodes technisch beheerd kunnen worden, dient te voorzien in functionaliteit om netwerknodes en hun actuele systeemconfiguraties te registreren.
NW-19.2	De centrale netwerk beheervoorziening, waarmee netwerknodes technisch beheerd kunnen worden, dient te voorzien in functionaliteit om de (actuele) operationele status van netwerknodes te monitoren. Zowel het actief als passief monitoren van netwerknodes op basis van in de markt gangbare open standaarden (e.g. SNMPv3) moet hierbij mogelijk zijn.
NW-19.3	De centrale netwerk beheervoorziening, waarmee netwerknodes technisch beheerd kunnen worden, dient log-data van netwerknodes o.b.v. in de markt gangbare protocollen (e.g. syslog, CEF) te kunnen ontvangen en opslaan voor nadere analyse.
NW-19.4	De centrale netwerkbeheervoorziening, waarmee netwerknodes technisch beheerd kunnen worden, dient protocollen (e.g. SFlow, NetFlow, IPFIX of gelijkwaardig) te ondersteunen waarmee informatie m.b.t. analyse van het netwerkverkeer verzameld kan worden.
NW-19.5	De centrale netwerk beheervoorziening, waarmee netwerknodes technisch beheerd kunnen worden, dient te voorzien in functionaliteit om op afstand: • netwerknodes te voorzien van softwarematige beveiliging- en systeemupdates, • de technische configuratie van netwerknodes te backuppen, • de technische configuratie van netwerknodes te restoren, • de technische configuratie van netwerknodes af te dwingen (via in de markt gangbare open standaard protocollen (e.g. TLSv1.3, SSHv2, NETCONF, RESTCONF of gelijkwaardig)).
NW-19.6	De centrale netwerkbeheervoorziening, waarmee netwerknodes technisch beheerd kunnen worden, wordt vormgegeven via een fysieke appliance of virtual machine (i.e. VMWare ESXi) appliance.
NW-19.7	De centrale netwerkbeheervoorziening, waarmee netwerknodes technisch beheerd kunnen worden, dient te voorzien in functionaliteit waarmee rapportages kunnen worden verkregen over: • actuele hard- en softwarematige configuraties van netwerknodes, • operationele status van netwerknodes, • historische data over de prestatie van netwerknodes.
NW-19.8	Bij uitval van (functionaliteit van) de centrale netwerk beheervoorziening is er geen impact op het operationele functioneren van netwerknodes in de infrastructuur.
NW-19.9	De centrale netwerkbeheervoorziening, waarmee netwerknodes technisch beheerd kunnen worden, dient te voorzien in een web-based gebruikersinterface waarmee de voorziening functioneel beheerd kan worden. Er geldt dat: • Toegang tot de web-based interface is beveiligd door authenticatie van user credentials van beheerders tegen de centrale directory service (van de IAM-omgeving) van de gemeente. • Autorisatie van beheerders tot functionaliteit gebeurt o.b.v. RBAC (least privileged access). • Audit logs worden bijgehouden van alle beheeractiviteiten.

Bijlage B: Gebruikte afkortingen

Afkorting	Verklaring
ABB	Architectuur BouwBlok
ANSI	American National Standards Institute
CoPP	Control Plane Policing
FO	Functioneel ontwerp (ook wel high-level design)
HLD	High-level lesign (ook wel functioneel ontwerp)
IEEE	Institute of Electrical en Electronics Engineers
IAM	Identity & Access Management
IdP	Identity Provider
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISSU	In-Service Software Upgrade
(DC-)LAN	(Datacenter) Local Area Network
LLD	Low-level design (ook wel technisch ontwerp)
MAB	MAC Authentication Bypass
NAC	Network Access Control
OOB (management)	Out-of-band (management)
PEP	Policy Enforcement Point (e.g. een netwerk firewall)
RBAC	Role-based access
SCEP	Simple Certificate Enrollment Protocol
SDN	Software-defined networking
SGT	Scalable Group Tag (ook wel Security Group Tag)
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SSH	Secure Shell
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
TO	Technisch ontwerp (ook wel low-level design)
WPA	WiFi-Protected Access